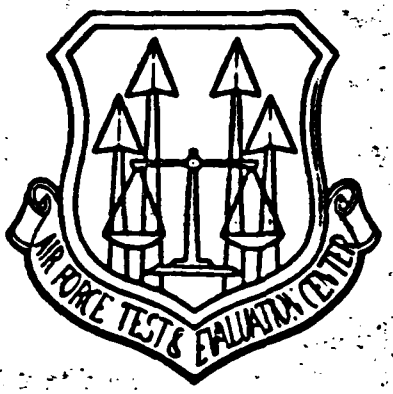
IV-34

1

COL. GERRISH



ELECTRONIC WARFARE SYSTEM OPERATIONAL TEST AND EVALUATION

MARCH 1980

Approved for public release; distribution unlimited.

AIR FORCE TEST AND EVALUATION CENTER
KIRTLAND AIR FORCE BASE
NEW MEXICO 87117

IV-34

ELECTRONIC WARFARE SYSTEM OPERATIONAL TEST AND EVALUATION

FINAL REPORT

MARCH 1980

Prepared by: JOHN F. NAGEL, Col, USAF
Director of Analysis

WILLIAM D. FARMER, Capt, USAF
Chief, Special Support Branch

Approved By: HOWARD W. LEAF, Major General, USAF
Commander

Approved for public release; distribution unlimited.

AIR FORCE TEST AND EVALUATION CENTER
KIRTLAND AFB, NEW MEXICO 87117

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER	2. GOVT ACCESSION NO. AD-A130674	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) ELECTRONIC WARFARE SYSTEM OPERATIONAL TEST AND EVALUATION		5. TYPE OF REPORT & PERIOD COVERED Final
		6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) WILLIAM D. FARMER, Capt, USAF JOHN F. NAGEL, Colonel, USAF		8. CONTRACT OR GRANT NUMBER(s) N/A
9. PERFORMING ORGANIZATION NAME AND ADDRESS Air Force Test and Evaluation Center (AFTEC) Kirtland AFB, NM 87117		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS N/A
11. CONTROLLING OFFICE NAME AND ADDRESS AFTEC/OA Kirtland AFB, NM 87117		12. REPORT DATE March 1980
		13. NUMBER OF PAGES
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office) N/C		15. SECURITY CLASS. (of this report) Unclassified
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

N/A

18. SUPPLEMENTARY NOTES

N/A

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Electronic Warfare (EW), Operational Test and Evaluation (OT&E)

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

This paper addresses some of the challenges and problem areas which confront operational testers attempting to assess the effectiveness of electronic warfare (EW) systems and provide information necessary for the decision making process. The paper points out the necessity of using analytical models and hybrid laboratory simulators with field testing in a comprehensive test and evaluation program and proposes that such a methodology be accepted as the standard approach to EW OT&E. The paper also identifies requirements for developing → cont.

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

cont → basic test facilities for EW system evaluation. It is emphasized that the approach is also applicable to other phases within the life-cycle of the EW systems, i.e., development, tactics evaluation, training; hence, test facility development and operation must be a coordinated Air Force effort.

EXECUTIVE SUMMARY

Introduction.

The assessment of the effectiveness of any combat-related weapon system through operational test and evaluation (OT&E) is difficult at best, and assessment of the effectiveness of electronic warfare (EW) systems is certainly among the most difficult. This paper describes an approach for OT&E of EW systems which, if properly employed, could significantly improve the evaluation process. Although the approach discussed is generally applicable to all aspects of EW, this paper limits the discussion to systems used for defense suppression. The approach described for OT&E has considerable application for developmental test and evaluation (DT&E). Additionally, the using commands can use the same methodology for evaluation of operational concepts and tactics.

EW OT&E poses many problems, several of which are not encountered during OT&E of other weapon systems. The principal measure of merit for defense suppression systems is their contribution to the survivability of attack aircraft, and successful completion of the attack mission. However, in EW OT&E, there are no "bodies to count" or "holes in the ground." How then does the EW tester actually measure the contribution of EW systems to survivability and mission accomplishment? Often the EW system operation is not well defined until late in the development process. Doctrine for operation of threat systems is not well known. Current test facilities, including threats, instrumentation, communication, and data management systems are generally inadequate.

EW OT&E: Past and Present.

In the past, acquisition decisions for EW equipment have been made based on test results of engineering measurables--radiated power, detection times, etc.--as defined in contractual specifications. However, in 1976, beginning with the F-4G Wild Weasel OT&E, the OSD

Deputy for Research and Engineering (OSDDRE) began requiring operationally meaningful evaluation measures. Accordingly, operational evaluation criteria were developed by AFTEC for the F-4G W/W, EF-111A tactical jamming system and the ALQ-131 ECM pod. Decision makers want to know the incremental contribution to total force structure of a new EW system. This is a force-on-force issue. The EW tester is usually limited to one-on-one or at best, few-on-few testing conditions. He must have a methodology to bridge this gap.

Partitioning the Problem.

EW systems used for defense suppression can generally be partitioned into two categories according to the basic role of the EW system. Some are supportive and attempt to reduce the chance of the aircraft being engaged; others provide self-protection and are designed to reduce the kill potential once an engagement occurs. This partitioning is the initial step in the methodology for evaluating EW system effectiveness. Testers cannot collect, directly from testing, the data required to address the overall success of the combat mission. Therefore, it is necessary to "back off" from the desired measurement to some lesser level of data which can be obtained from testing. Extrapolation techniques are then required to take results from small-scale test events and project what the results would be in a "real life" combat scenario.

Tools for Testing.

The basic tools available to EW testers generally take the form of field test ranges, hybrid man-in-the-loop simulators, and analytical models. The field ranges such as those at Eglin AFB, FL, and Nellis AFB, NV, are well known. There are several hybrid simulators; the two best known and most often used by the Air Force are the Air Force Electronic Warfare Evaluation Simulator (AF-EWES) and the Real-Time Electromagnetic Digitally Controlled Analyzer and Processor (REDCAP). The analytical models referred to here are large-scale computer simulations. The applicable models for direct use in testing range from

one-on-one to many-on-many. Results from these models ultimately provide input for force-on-force models for the final phase of evaluation.

For various reasons, no single one of these tools by itself is adequate to provide a comprehensive evaluation. For example, a hybrid man-in-the-loop simulator such as AF-EWES can provide a capability to test against newer threats sooner than those threats can be developed for field use. Hybrid simulators are cheaper and safer. The field ranges are required for a wider range of action and reactions by both aircraft and ground threat system operators. Simulation, both digital and hybrid, can provide a means for efficient test planning. Additionally, as digital simulation models are validated with empirical data from testing, they can be used for evaluation of the system under test in a more dense and complex threat environment, where one tool is weak, another may be strong. By using all the tools, an EW tester can do a more complete job of testing. The integrated methodology is shown in figure 1. It can be summarized as:

- Initial modeling phase for sensitivity analysis and test planning.
- Active test phases at hybrid laboratory simulator and field range facilities.
- Test data reduction and analysis.
- Post-test modeling phase repeating the first step using test data for extrapolation.
- Force effectiveness modeling and analysis phase to determine the incremental contribution of the new system to total force effectiveness.

This concept was used to some degree during the EF-111A IOT&E. Although it was not preplanned, it did evolve. All the tools were used. During the EF-111A program reviews, OSD personnel stated that the operational effectiveness evaluation of the EF-111A was the most comprehensive OT&E to date of any EW system.

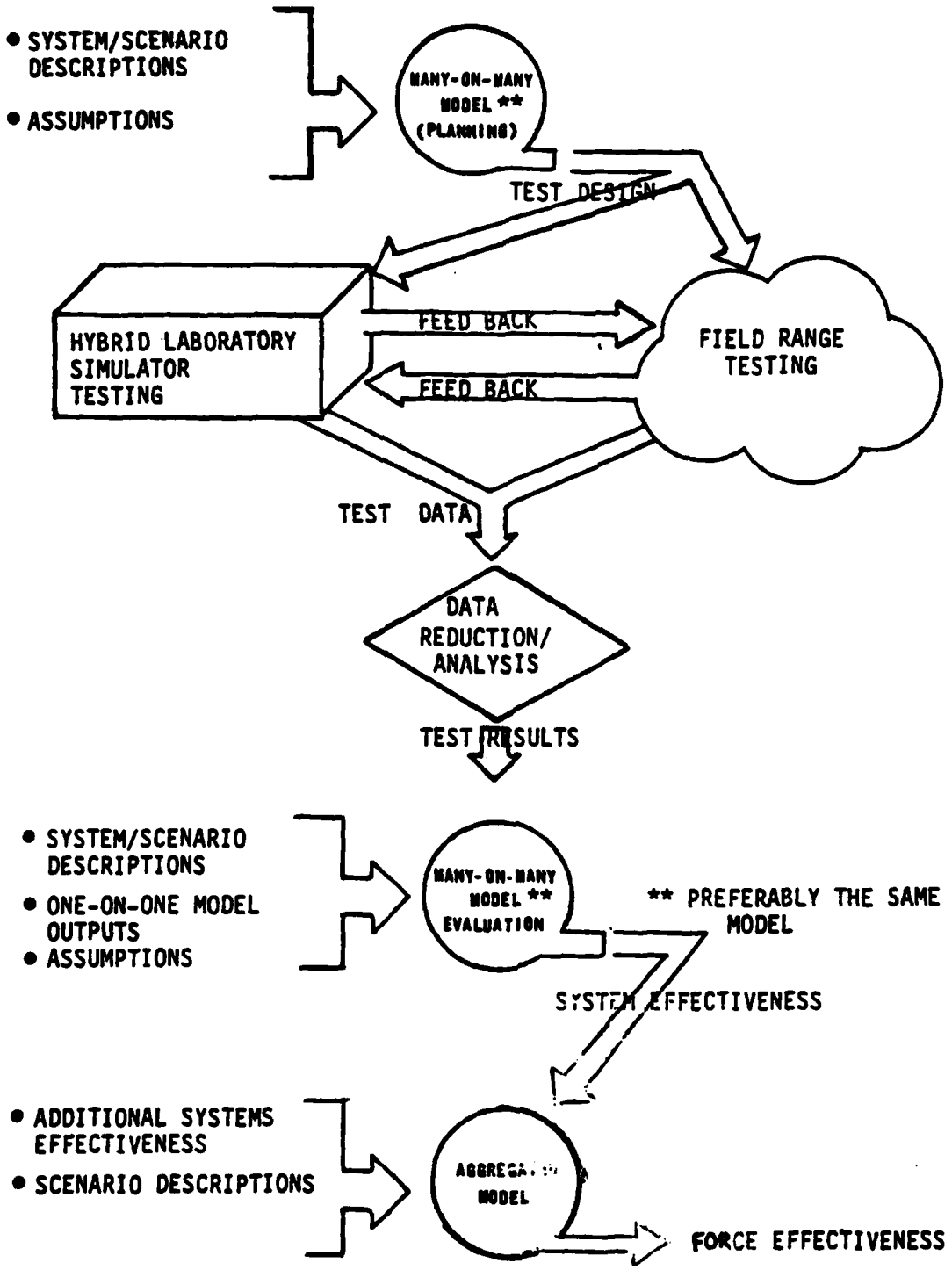


Figure 1. Integrated EW OT&E Approach

Required Test Environments.

Improvements are required in both the field EW ranges and hybrid man-in-the-loop simulators. Improvements are required in numbers and types of threat system simulators, validation of simulators, operation with correct doctrine, instrumentation, and data management systems. Overall goals should be established for developing test facilities rather than the current process of providing improvements on a case-by-case basis for individual EW system test programs. Consequently, any improvements to the test facilities should be the concern of all. It should be pointed out that the same facilities used by the OT&E community are used by the developers (AFSC) and operational commands (SAC, TAC, etc.). The operating commands currently use the field test facilities for tactics development and training. It is envisioned that with improvements to the hybrid simulators, the operational commands can also use these facilities for tactics and concept exploratory trials. To insure the test facilities meet all the users' needs as much as possible, all should participate in planning their improvements and funding their subsequent operation.

Summary/Recommendations.

The OT&E methodology proposed in this paper is one which uses analytical models and hybrid laboratory simulators with field testing to achieve a more comprehensive assessment of an EW system. The current test facilities (field ranges and hybrid laboratory simulators) are not adequate to support OT&E of evolving EW systems. Improvements to hybrid laboratory simulators such as AFEWES need firm direction. The recommendations for AFEWES presented in this report provide a basis for a master plan. Improvement of the test facilities should be an equal concern of AFSC, TAC, SAC, and AFTEC since all benefit and are users. Implementation and acceptance of the proposed evaluation methodology and the needed improvements to facilities require support at the highest levels in the Air Force.

IV-34

CONTENTS

FIGURES

IV-34

TABLES

TABLES

ABBREVIATIONS

AAA	Antiaircraft Artillery
AAM	Air-to-Air Missile
ACI	Airborne Controlled Intercept
ADU	Air Defense Unit
AFB	Air Force Base
AF-EWES	Air Force Electronic Warfare Evaluation Simulator
AF/SA	Air Force Studies and Analysis
AFTEC	Air Force Test and Evaluation Center
AI	Airborne Intercept
CAS	Close Air Support
DSARC	Defense System Acquisition Review Council
DT&E	Development Test and Evaluation
ECCM	Electronic Counter-countermeasure
ECM	Electronic Countermeasure
EMTE	Electromagnetic Test Environment
EW	Electronic Warfare
EWJT	Electronic Warfare Joint Test
FAA	Federal Aviation Administration
GAO	General Accounting Office
GCI	Ground Controlled Intercept
GPS	Global Positioning System
IDIP	Intelligence Data Input Package
IOT&E	Initial Operational Test and Evaluation
JCS	Joint Chiefs of Staff
MHz	Megahertz
MOE	Measure of Effectiveness
OSD	Office of the Secretary of Defense
OSDDRE	Office of the Secretary of Defense, Deputy for Research and Engineering
OT&E	Operational Test and Evaluation
P_e	Probability of Engagement
P_k	Probability of Kill
PLSS	Position Location Strike System
PRF	Pulse Repetition Frequency

ABBREVIATIONS (continued)

QRC	Quick Reaction Capability
R&D	Research and Development
REDCAP	Real-time Electromagnetic Digitally Controlled Analyzer and Processor
RF	Radio Frequency
RWR	Radar Warning Receiver
SAM	Surface-to-Air Missile
SPO	System Program Office
TACOS	The Air Combat Operations Simulation
TADBM	Tactical Air Defense Battle Model
TJS	Tactical Jamming System
TSPI	Time-Space-Position Information
US	United States
WW	Wild Weasel

SECTION I

INTRODUCTION

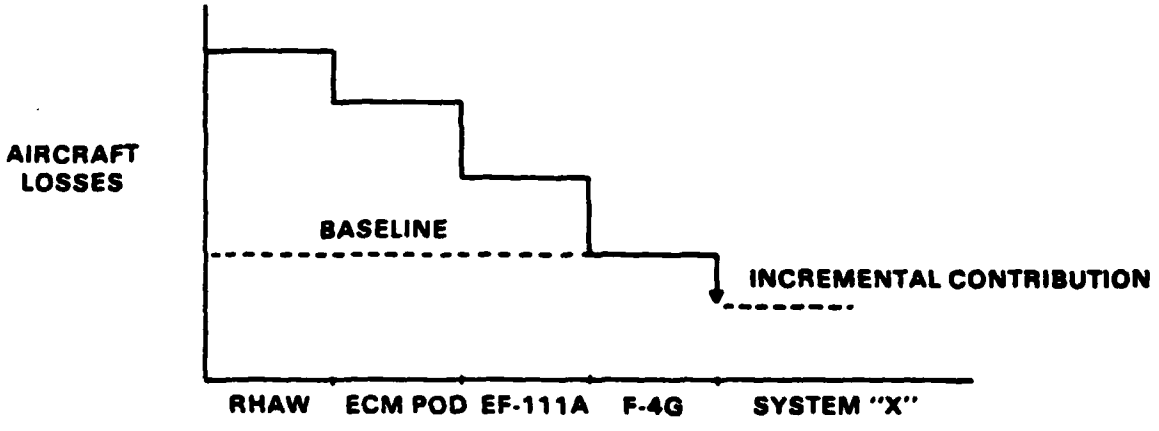
> "Electronic Warfare (EW)," as defined in JCS Pub. 1, "is military action involving the use of electromagnetic energy to determine, exploit, reduce, or prevent hostile use of the electromagnetic spectrum and action which retains friendly use of the electromagnetic spectrum."

The Air Force currently has underway several high level management initiatives to resolve what are generally conceded to be major problems in developing an effective EW capability. This paper will concentrate on operational test and evaluation (OT&E), one of the most difficult and important areas needing attention.

From the above JCS Pub. 1 quotation, one can see that there are many operational aspects to EW. In general, however, what comes to mind most often is defense suppression--both lethal and nonlethal. By far the largest and most important EW efforts are expended in this area. Although the discussion in this paper will primarily address OT&E of the effectiveness of defense suppression systems, with little change it would be equally applicable to the other aspects in the life-cycle of EW systems. For example, research and development (R&D) activities and efforts to develop tactics frequently face the same problems which confront OT&E. Solutions to those problems which improve the quality of OT&E can also benefit the developers and the ultimate users of EW systems. Hence, while this paper addresses OT&E, expressions like "tester" can usually be replaced by "developer" or "user" with little or no loss of meaning or emphasis.

The assessment of the effectiveness of any combat-related weapon system through OT&E is difficult at best, and assessment of the effectiveness of EW systems is certainly among the most difficult. Find someone who disputes either of these two statements and you will have someone who has never been involved in OT&E. Consider the following questions which must be addressed in OT&E of defense suppression

systems. How does one measure, determine, or estimate the level of attrition reduction which can be attributed to EW? And, since there is a proliferation of EW systems, each contributing in some way (as illustrated in figure 2) how does one isolate the incremental effects of any one EW system? What is the relative difference between the effects of support jamming and the effect of information provided to the aircrew member by the radar warning receiver? What is the absolute difference between the effects of self-protection jamming and the effects of anti-radiation missiles?



NOTE - A NOTIONAL PRESENTATION NOT INTENDED TO INDICATE ORDER OR RELATIVE EFFECTIVENESS

Figure 2. EW Contribution to the Defense Suppression Objective

EW OT&E poses many problems, several of which are not encountered during OT&E of other weapon systems. Other than with lethal defense suppression systems such as the F-4G Wild Weasel (WW) and the Precision Location Strike System (PLSS), which are directly related to an ordnance delivery capability, there are no "holes in the ground" or other physical damage which can be used as a direct measure of the system's worth. However, even with the F-4G WW and PLSS, the lack of emitter density in type and numbers on a test range precludes a thorough OT&E and the subsequent development of tactics. Moreover, the class of EW systems generally referred to as electronic countermeasures (ECM), the systems which don't put holes in the ground--jammers, warning receivers, chaff, flares, etc.--accounts for the vast majority of the EW OT&E effort. Whether an EW system is intended to provide self-protection to the carrier aircraft, ECM support to other aircraft, or even destroy a ground-to-air or air-to-air defense system, the ultimate measures of merit for operational effectiveness must be survivability of the attack aircraft and their opportunity to complete attacks. However, in OT&E, just as in tactics development and training, no surface-to-air missiles (SAMs), antiaircraft artillery (AAA) rounds, or air-to-air missiles (AAMs) are actually fired at the attacking aircraft, nor are any defense systems occupied with operators actually fired upon. Thus, lacking the realism of "bodies to count" and "holes in the ground," how does the EW tester adequately address the EW contribution to the mission?

Designing an OT&E to credibly determine military utility has been historically constrained by an incomplete knowledge of just how a system will eventually work and, more important, how it should be employed. The very nature of EW has frequently caused it to be referred to as "part science, part art." Whether or not an employment technique or internal process of an EW system will work is often dependent upon the skill of the operator of the intended victim system. Frequently the tester can learn only through trial and error just what he should be testing for. About the only thing an OT&E tester can be sure of at the beginning of a test is that the results from controlled developmental testing, the engineering measurables, will not be adequate to address

all OT&E considerations. Without a good definition of what a system is and how it should be employed, how does the tester design and conduct sufficient OT&E?

Countermeasures development is at best a "catch up" process. The development of EW systems is dependent upon and, consequently, lags our technical knowledge of the threat environment in which the system must operate. Defense suppression EW systems are developed to counter known enemy threat systems. To counter this lag in intelligence of newly deployed threats, EW systems are now developed to be software programmable. This development offers some opportunity to respond, but still an EW system tends to approach obsolescence by the time it is fielded in quantity. The current wave of concern over our newest systems' capabilities to counter known Soviet ECCM capabilities illustrates the lag which exists between system development and deployment and the threat to be countered. Early definition of a threat, that is a technical description of system performance, is only part of the problem. Much of the effectiveness of EW systems is dependent upon the real-time decisions and actions of threat system operators which are based upon operating doctrine, tactics, and procedures which may not be known. In fact, it is unlikely that these elements are known with sufficient detail or confidence to permit development of a realistic simulated threat environment even when hardware is available. How then does the tester determine the effectiveness of the EW system in its intended operating environment?

Finally, the development of adequate facilities for testing even lags the capabilities of our newly evolving EW systems. A major problem, of course, is the timely development of threat simulators for the test facilities. But inadequacies in the test facilities cover a broader spectrum than just the lack of a representative threat environment. They also include deficiencies in instrumentation, communication, and data management systems which are essential components of any EW OT&E program. As EW system complexity increases to counter rapidly advancing threat system capabilities, the sophistication required in test facility support systems also increases. How then does the tester compensate for those range inadequacies and provide an assessment of EW system effectiveness in the threat environment in which the system will operate?

The basic problems which have been identified will continue to confront anyone attempting to evaluate the military worth of an EW system. Threat system density, diversity, and complexity continue to increase; EW systems designed to counter them are becoming more sophisticated, complex, and expensive; and operational testers are being pressured to provide more timely, credible, and operationally meaningful effectiveness data to support the decision making process. It is essential that operational testing of EW systems be structured to be responsive to that challenge. Billions of dollars are being spent to develop and procure EW systems. We can't afford to fill the "shelves" with the wrong systems. We can't afford it in money, and the aircrews can't afford it in war.

The purpose of this paper is to describe an approach to EW OT&E which can help solve or at least mitigate somewhat the problems confronting the tester and the decision maker and to identify some basic actions which will be required to make the approach work. It is an approach which has application throughout the life-cycle of the EW system; research and development, developmental testing, operational testing, and tactics development. The approach stresses the integrated use of analytical models and hybrid laboratory simulators in conjunction with field testing to assess the operational effectiveness of EW systems. The concept is neither new nor unique. In a sense, such an approach was attempted (with little success) during the Electronic Warfare Joint Test (EWJT) in 1974. The idea has been advocated in numerous studies, reports, papers, briefings, and test designs during the past few years, but acceptance has been slow. What has been lacking is a successful application to add impetus to its use. Recently, however, the Air Force Test and Evaluation Center (AFTEC) implemented the concept with moderate success during the EF-111A initial operational test and evaluation (IOT&E) in 1978. In advancing or proposing a new or revised way of doing something, it is implied that the existing or former procedure fell short of its goal. That is clearly the case with EW OT&E, and this paper identifies deficiencies with the current process and identifies major areas that need improvement. Resource limitations contribute substantially to incomplete and inadequate effectiveness assessments on test ranges, and there is a natural reluctance to use

simulation results as part of an operational evaluation. Test facilities will most likely continue to be resource limited, but their development should be approached with some long-range goal in mind.

Identifying the deficiencies of a procedure or method of doing something is only part of the problem--often the simplest part. Developing a better approach is a more difficult task, but implementing it is an even greater challenge. Successful implementation of the methodology proposed in this paper will require an Air Force commitment to accomplish more credible EW system OT&E. Taking the approach proposed in this paper will make the proposed methodology work, and they are all achievable.

The authors have approached the task of preparing this paper with more than a small feeling of apprehension. We have been close to EW system testing for several years and recognize it as a very difficult and complex business. We were concerned that the level of detail which could be presented in this forum may appear to be a rather trivial treatment of the problem. However, our continuing experiences in study groups, test planning meetings, and other philosophical discussions have reaffirmed our conviction that some common level of awareness is required. Before we can begin to attack and solve the problems which confront us, we must at least share an understanding of those problems. There must also be some basic recognition of the requirements for getting well and a commitment to do so. This then has been our principal objective, to provide a baseline from which we can effectively communicate and begin the process of improving the way we develop, test, and evaluate the effectiveness of electronic warfare systems.

SECTION II

EW OT&E: PAST AND PRESENT

In the past, acquisition decisions for EW equipment have been made based on engineering measurables--radiated power, detection times, etc.--as defined in contractual specifications. The decision makers were not presented with test results or evaluations based on testing which translated technical performance into operationally meaningful results. This situation was dictated largely because the engineering measurables were available and there was no accepted methodology for translating the engineering measurables into effectiveness results which were operationally meaningful.

Using engineering measurables as being sufficient criteria for acquisition decisions is easily challenged. The evolution of an EW system generally begins when one of the major operating commands issues what was formerly called a required operational capability and is now called a statement of operational need. The developer must translate a "capability" or "need" into a set of detailed specifications which defines a very specific piece of equipment. A contractor may in fact build a system meeting or exceeding the contractual performance requirements. However, meeting specifications in no way guarantees that the system's performance will achieve the desired defense suppression results. The OT&E tester must devise an OT&E which will bridge the gap between the engineering measurables and the performance described in terms of military utility, the system's contribution to defense suppression.

In fact, until recently very little in testing procedures or the issues required to be addressed for EW system acquisition had changed since the quick reaction capability (QRC) days of the Vietnam era. For testing procedures, it is true that planning had improved and more realism had been sought in the test environment. However, the acquisition issues, and, consequently, the reported test results, were generally still limited to engineering measurables.

A significant change in the acquisition issues for EW systems occurred in 1977 within the Office of the Secretary of Defense (OSD). By late 1976 it had become apparent to AFTEC that engineering measurables, specifications, were not adequate to address military utility of weapon systems. This was particularly true with EW systems. The F-4G Wild Weasel which was under development at the time was selected by the AFTEC Commander to be used as a model for formalizing an approach for using operationally relevant criteria for T&E. Both the SPO and contractor accepted the criteria as essential guidance for completion of the developmental effort. During the IOT&E, which was completed in February 1977, the F-4G Wild Weasel was evaluated using the operational criteria. Results were reported to OSD and a favorable production decision was made. Participating OSD personnel considered the operational criteria to be a significant improvement in how test results were reported. It was no longer "business as usual." As a result of this experience OSD is taking a closer look at EW OT&E's and is focusing on operationally meaningful evaluation criteria. The next major EW program being considered by the Air Force was the EF-111A tactical jamming system (TJS). OSD wanted to know how many aircraft the EF-111A saved--not just how many watts/MHZ were radiated. Further, OSD directed additional operationally relevant testing be accomplished with the ALQ-131 ECM pod. The results of OT&E had become significantly more critical for production decisions.

Today the operational tester of EW systems is confronted with an "ultrarealism syndrome." The requirement for testing to be conducted under representative operational scenarios is generally accepted, but the current quest for absolute realism will remain elusive. Air Staff, OSD personnel, General Accounting Office (GAO) representatives, and Congressional Staff members all want more and more realism in the test environment. Everyone would like to have test results which could be directly used to address real life. However, neither the desert environment around Nellis AFB, nor the shore line at Eglin AFB provide realistic representations of the Fulda Gap in Central Europe occupied by a Soviet Combined Arms Army. Full-scale replica simulators are considered essential to EW OT&E, and absolute threat system density is

regarded as a must. However, the realism of threat density most often degrades to one-on-one or at best few-on-few conditions. Many observers believe only flight testing provides genuinely credible results. Testers want realism as much as anyone, but the level of realism required is that which provides a credible representation of the expected operational environment; and that cannot always be achieved in a field test environment.

The scale of testing, unlike the questions to be addressed, is usually small as illustrated in figure 3. The decision maker, being asked to make a multi-million dollar production decision on a newly developed EW system, would like to know how that system will affect total force structure. This request seems reasonable. However, during the EF-111A IOT&E, the "operational" test was limited to no more than a single support jamming system escorting a four-aircraft attack force striking a target complex defended by a handful of surveillance and tracking radars. Prototype systems are in short supply for testing, operational assets are difficult to acquire from the operating commands, threat system simulators (both type and density) are as scarce as prototype EW systems, and the simultaneous availability of more than a single type of EW system for testing is a rare occasion to be treasured. To some extent, joint operational tests tend to rise above the one-on-one constraints and may approach few-on-few conditions. The reason is rather straightforward. They are not usually evaluations of prototype systems but tend to assess proposed or previously untried tactical concepts. Operational systems are usually available from the services and threat simulator assets are brought together temporarily to enhance test environment realism. However, for new system development, because of the limited availability of test resources, and high program cost EW OT&E is generally limited to not much more than one-on-one conditions, while the decision maker's interest is usually at the many-on-many level.

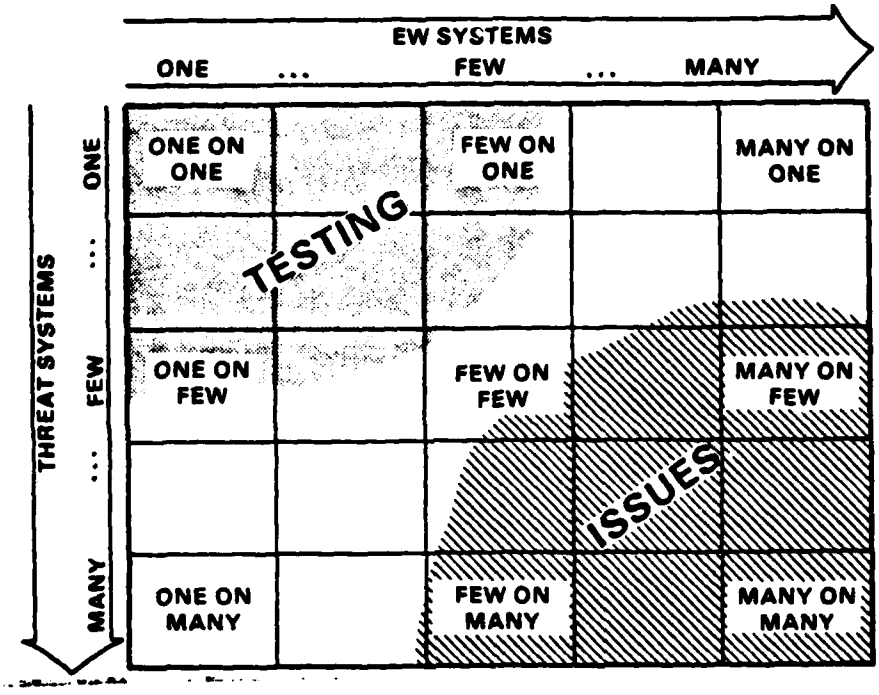


Figure 3. Testing and the Issues: Ends of the Scale

There is a danger at this point to come down hard on the EW tester believing he is making excuses. As has been pointed out, operational testing of EW systems provides several dilemmas which are never completely solved and rarely even alleviated. Remember that the ultimate measure of an EW system's operational effectiveness must be based upon the overall success of the combat mission. The tester must deal with and overcome many criticisms and biases when departing from the ultimate realism which is desired. Realism is expensive, and the operational tester is caught in the middle. Although typically constrained to a budget which he does not control, the tester must ultimately make the tradeoffs between test objectives and test costs. The rationale for those decisions must be fiscally defensible, even though it still may not be operationally acceptable.

The operational tester also has a problem in dealing with the developer. Unless the developer is blessed with an extraordinary measure of luck, his new system usually suffers through a great deal of growing and maturing "pains" during development testing. The operational tester also suffers because the additional development time is almost always at the expense of operational testing. It is ironic that development testing is considered an "integral part of" the development process, but operational testing is generally regarded as a "disruption to" that same process. Even when the new system is finally turned over to the operational tester, the developer may not be finished with it. He wants to continue refining its operation so that the system works as best it can when decision time arrives. That isn't all bad, but it does make it difficult to accomplish operational testing with any semblance of a stable system configuration.

SECTION III

PARTITIONING THE PROBLEM

EW systems used for defense suppression can generally be partitioned into two categories according to the basic role of the EW system as shown in figure 4. The probability of an aircraft loss can be approximated by the product of the probability of engagement and the probability of kill given that an engagement has occurred. Systems like the EF-111A, the F-4G, and the PLSS are in the former category, are generally supportive, and attempt to reduce the chance of aircraft engagement. Self-protection systems such as the ALQ-131, flares, chaff, and radar warning receivers (RWRs) are designed to reduce the kill potential once an engagement occurs. Tactics, of course, must be recognized as a major factor overlaying both of these two broad EW system categories. It is especially important that the EW system's effects on the defense system and the employment tactics be compatible. For example, there is little value in providing a noise jamming strobe to a surveillance radar while attempting to avoid detection by flying at low altitude to optimize the effects of terrain masking.

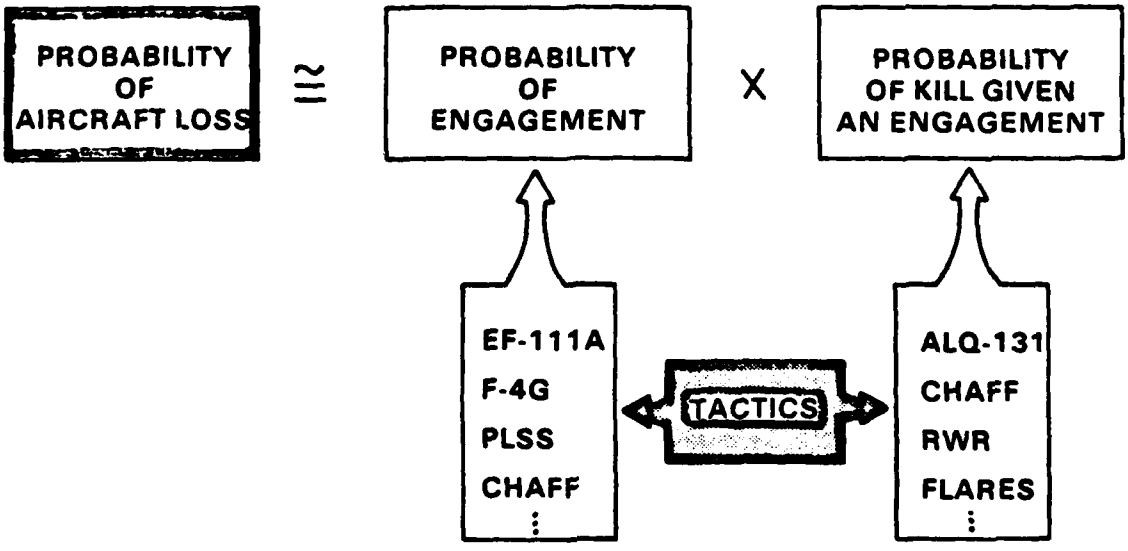


Figure 4. EW System Partitioning

Partitioning of the EW systems according to their role is the first step toward determining a procedure for measuring effectiveness. It is a step of necessity more than convenience because the true measure of effectiveness (MOE) must be concerned with the overall success of the combat mission. Hence, an appropriate measure of the EF-111A's support jamming effectiveness would be the change in attrition of attack aircraft being supported by the EF-111A. That was, in fact, the principal MOE during the EF-111A IOT&E conducted by AFTEC. But EW testers haven't always thought of MOEs at that level and still cannot collect the required data directly. The tester must "back off" from the desired measurement to some lesser level of data which can be obtained from testing.

Generally there is a reasonably, well-ordered heirarchy of data elements required to determine an aircraft's kill probability. For example, for a SAM they include:

- Aircraft detection/burnthrough.
- Target lockon.
- Missile firing.
- Radar tracking error.
- Missile trajectory.
- Fuzing mechanism.
- Warhead fragmentation pattern.
- Aircraft damage.

The tester cannot get much closer to his goal, directly from testing, than determining tracking error. And that depends heavily on good instrumentation. Test measurements tend to observe detection/burnthrough events, determine tracking errors, and count aircraft engagements by the defense systems. Computer models may then be used to determine a probability of kill for each missile firing event. The process is certainly not universal, and many test results are presented without extrapolation or evaluation. Extrapolation, in this context, and as depicted in figure 5, refers to taking results from small-scale test events and, through analysis techniques, projecting what the results would be in a "real life" combat scenario.

IV-34

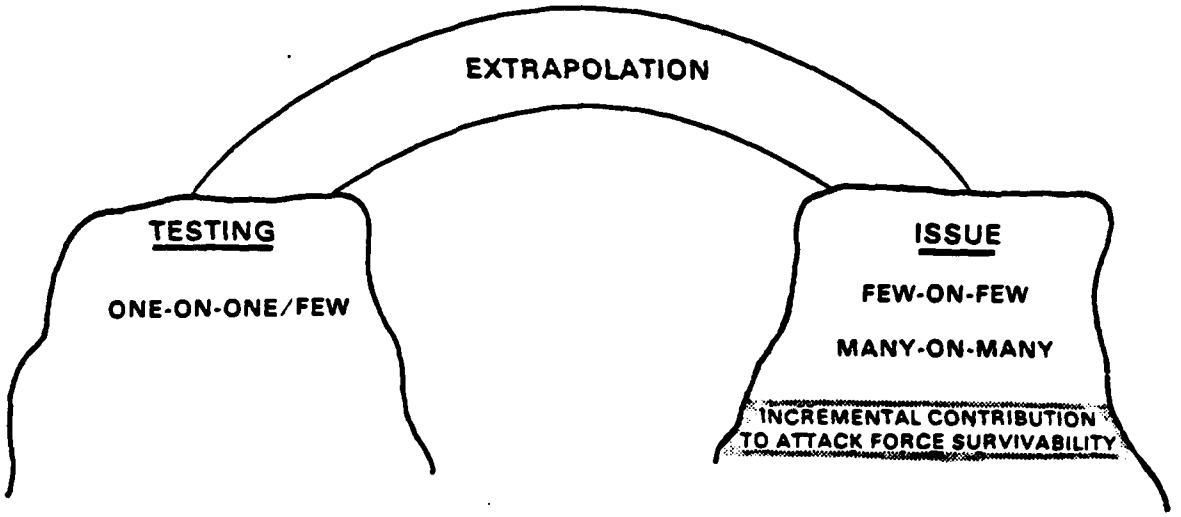


Figure 5. Addressing the Issue

The extrapolation procedure is neither simple nor well understood and, consequently, seldom successfully accomplished. The tester is strongly tempted to ignore it and just present the test results; this temptation must be avoided. Extrapolations which have been attempted as part of EW OT&E have generally failed in two critical areas: they have tended to be linear, and the contributions of multiple EW systems have usually been assumed to be additive. Neither assumption is valid; both result from failure to use or ineffectively using analysis tools such as simulation. The linearity assumption is perhaps one of convenience rather than deliberateness. Engagement rates for one air defense unit (ADU) are indiscriminately applied to all ADUs, and the ratio of aircraft engaged from a small formation is considered to be the same as that for a large formation. Obviously, such assumptions are faulty, but they are examples of the hasty generalizations which occur. Most EW testers would readily agree that the approach is not correct, and they would do it differently if time and talent permitted.

The assumption that EW effects are directly additive is much more subtle and potentially misleading. Its application is much more widespread, and its fallaciousness is perhaps more readily recognized by EW testers. However, there is not a great deal of knowledge and experience at dealing with the problem. It requires recognition and understanding of the cooperative, complementary, and/or cumulative effects of multiple EW systems, the synergisms which exist among various EW systems.

It seems appropriate at this point to determine what is really meant by synergism. The expression has become quite popular during recent years; it is not properly understood, and the word has often been misused. Synergism is defined as the "cooperative action of discrete agencies such that the total effect is greater than the sum of the two effects taken independently." Is this what we really mean or expect when speaking of the synergistic effects between the EF-111A and the F-4G? Perhaps such an effect cannot really be achieved, and we don't expect it anyway. On the other hand, consider the medical definition of synergist which is described as "a remedy acting similarly to another remedy and increasing its efficiency when combined with it." Since dissimilar EW systems affect defense systems in ways which are not directly additive, perhaps a more realistic definition of synergism for EW, from a military point of view, would be "the cooperative action of discrete systems such that the individual effects are enhanced by the presence of the other thus enhancing successful achievement of mission goals." This definition seems to be more closely related to our real perception of synergistic effects. On the other hand, it is also necessary to describe the possible negative or degrading effects of multiple EW systems employed together. But there has been no "buzz word" to describe that phenomenon. Consider, if you will, "disergism" as "the cooperative action of discrete systems such that the individual effects are degraded by the presence of the other thus adversely affecting successful achievement of mission goals." The reader can probably recall examples which could be provided, but they would serve no constructive purpose. What is important, is that the combined effects, good or bad, of multiple types and numbers of systems have not adequately been accounted for in EW OT&E.

Surely, the lot of those tasked with assessing the operational effectiveness of newly developed EW systems is a difficult one. The threat is growing, the systems to counter it are becoming more sophisticated, and the gap between testing capabilities and desires is widening. The tester is being challenged to take data, measured at a level lower than desired, during a small-scale test and to express the results in a way that is relevant to the real issue. It is not an easy task, and it has not often been adequately accomplished in the past. If there is to be any substantial improvement in the future, the extrapolation process must be improved, and the capabilities of test facilities must be pushed to their limit.

SECTION IV

TOOLS FOR TESTING

There is a general feeling within the EW community that EW system testing lacks credibility. It is especially true of operational testing partly because of the problem areas identified in the preceding sections. But part of the problem rests with the testers themselves who have been unaware, unwilling, or unable to adequately use the tools which are available for EW OT&E. Recognition of this is the first step to improving EW OT&E. Everyone associated with EW OT&E--testers, decision makers, and critics--must understand the capabilities and limitations of the basic EW test tools and how they can and should be used in an integrated approach.

Basic Tools.

The basic tools available to EW system testers generally take the form of field test ranges, hybrid laboratory man-in-the-loop simulators, and analytical models. Models, as envisioned here, vary in complexity and magnitude from simple equations to complicated large-scale computer simulations. The traditional "back-of-the-envelope" calculation can be considered a model. However, when thinking of models, we are most likely to envision large-scale computer simulations, and that is what is being considered here.

There are, of course, many levels of detail within models, ranging from those which describe specific events or processes in rigorous detail to those which generalize the effects of those events in describing their contribution to some larger process or occurrence. Models in the former category can be referred to as "system models," while those in the latter class are known as "aggregated models." An example of a system model is a SAM simulation which includes radar tracking, missile flyout, and miss distance calculated against a single target. There are many levels of aggregation. Generally, an aggregated model does not

address attrition based on individual engagements. One level of aggregation could be classes of defenses against classes of aircraft, i.e. SA-2 versus F-15, SA-2 versus F-16, etc. In this case a SAM system would have a probability of engagement (P_e) and a probability of kill (P_k) against each type of aircraft. Attrition would be computed by a model which included P_e, P_k, and the ratio of forces, a Lanchester equation. Aggregated models usually play several classes of defenses and attackers, both red and blue. The ratio of forces for various missions--close air support, air defense, etc.--can be based on a set strategy or can vary from raid to raid based on an optimization strategy. The effects of EW could be reflected in the P_k and P_e input data. The roles of various models used in the integrated methodology will be described in more detail in the next section.

Hybrid laboratory simulators may not evoke any immediate response from the reader, positive or negative. Nearly everyone has an opinion on analytical models; very few have experience with or, for that matter, even know what a hybrid laboratory simulator is. For this paper, the hybrid laboratory simulator is described as a radio frequency (RF) simulation using computer generated scenarios to drive hardware displays used by human operators. There are several facilities, but, for brevity, discussion is limited to two simulation facilities which have been developed (for the most part) by the Air Force for use in EW system testing: the Real-time Electromagnetic Digitally Controlled Analyzer and Processor (REDCAP), and the Air Force Electronic Warfare Evaluation Simulator (AF-EWES). Both are Air Force facilities. The REDCAP is located at and operated, under contract, by the Calspan Corporation, Buffalo, New York. The AF-EWES is located in Air Force Plant #4 and is operated, under contract, by General Dynamics, Fort Worth, Texas. Although some testing can be conducted against a few terminal defense systems, the REDCAP has been developed primarily to address ECM effects upon the relatively fixed, early warning network and the ground controlled intercept (GCI) system. The AF-EWES has been structured to permit evaluation of particular ECM systems against specific terminal threats. Though certainly not always the case, REDCAP can be generally considered as providing a "macro" assessment, while AF-EWES permits a "micro" evaluation.

Within the past two years, as a result of EF-111A testing, the AF-EWES has developed the surveillance and acquisition systems and the command and control structure associated with tactical SAM systems. In the past, both the REDCAP and the AF-EWES have been used during development testing; neither has been used extensively for operational testing, although they have great potential to support EW OT&E.

Field testing, unlike modeling and laboratory simulation, is reasonably well known. At least most people are familiar with the traditional test facilities. Most Air Force EW system testing has been conducted at the Electromagnetic Test Environment (EMTE) at Eglin AFB, and at the ranges around Nellis AFB in Nevada. The EMTE has provided an ample environment in which to accomplish development testing and some limited operational testing of self-protection systems where one-on-one testing is warranted. For operational testing of support systems (e.g., EF-111A, F-4G), the Nellis area provides the necessary airspace and best simulated threat environment. In the future, the Nellis Range is envisioned as a major training and test facility as a result of continuing development under the operational range improvement program. There are, of course, other facilities which the Air Force has used in the past and, along with others, will continue to be used for future testing. Most notable among them are the Naval Weapons Center's Echo Range, the White Sands Missile Range, and the Utah Training and Test Range.

Relative Comparison

Recognizing the tools available for EW OT&E is the essential first step. Understanding their relative advantages and disadvantages or strengths and weaknesses is next. Table 1 has been developed with this second objective in mind. Each of the three basic categories of test tools--models, simulators, and ranges--has been rated against several factors which impact the tester's capability to conduct effective and sufficient OT&E of defense suppression EW systems. Ratings of fair (F) or minimal, reasonably good (G), and very good (VG) have been assigned to models, simulators, and ranges for each applicable

factor. The ratings are intended to reflect the quality of a particular feature or capability of the class of test tool (not a specific model or facility) and represent the subjective assessments of the authors.

Table 1

Test Tool Comparison

TEST FACTORS	ANALYTICAL MODELS	HYBRID SIMULATOR	FIELD RANGE
1. Identify sensitivities	VG	G	
2. Test articles - number/ quality	VG/F	G/G	F/VG
3. Relative cost	VG(low)	G(med)	F(high)
4. Threat systems - number/ quality	VG/F	F/G	F/VG
5. Tactics - develop/evaluate	G/F	VG/F	F/VG
6. Configuration flexibility	G	VG	F
7. Environmental realism	F	F	G
8. Operator interface		F(one-sided)	G(two-side)
9. Hardware interaction		F(sub-system)	G(full-system)

One facet revealed in table 1 is the complementary nature of models, simulators, and ranges; where one is weak, another may be strong. For example, models and simulators can overcome the limitations on numbers of test articles available for testing. Hence, they receive more favorable ratings than the ranges where the numbers of available prototype systems are limited for flight testing. However, the few prototypes available for field testing are most often of much better quality than the mathematical representations used in models and simulators and, consequently, for quality, the range receives the more favorable rating. A similar argument can be made for the number and

quality of simulated threat systems in the ground environment. Also, models and simulators provide good vehicles for developing potential tactics and employment concepts, but the final evaluation of those tactics and concepts must be accomplished on the range. Operator participation is a strong feature of the simulator, but it is only one-sided--the red side--and field testing is required to achieve some level of interaction between red and blue forces. For purposes of discussion, the red side is operating the air defense system and the blue side is the aircraft attack force. However, there are sufficient limitations on the range so that even in the best test range environment all of the critical dynamic interactive processes which occur between aggressor and defender are still not realized.

The reader may not completely agree with these ratings and may choose to reevaluate the merits of models, simulators, and ranges against the indicated factors. You may even choose to add or delete factors from this list. Whatever you do, we believe you will conclude that the complementary features exhibited in table 1 emphasize the requirement to use all the tools--models, simulators, and ranges--to their full potential in a well-planned EW OT&E. It should be apparent that the benefits available to EW testers are also available to those who develop tactics: the opportunity to "try before fly;" the opportunity to work problems which cannot be worked on the range; and, in general, the opportunity to complete a more thorough and more meaningful evaluation.

Testers must recognize the capabilities and the limitations of the basic tools available for testing. Furthermore, there must be a dedicated effort to provide positive guidance for the continued enhancement and upgrade of those deficient tools which cannot adequately support the test and evaluation process. We have generally been content to pay no more than lip service to the deficiencies which confront us while dodging the problem by avoiding those facilities which are considered the most inadequate. Consequently, facilities are not improved, and we become more frustrated. We owe it to ourselves to exploit the capabilities of adequate test tools and to provide sound recommendations for resolution of deficiencies.

Testers must also adopt a positive approach to the use of laboratory simulator facilities. For too long we have regarded them as strictly DT&E facilities; and perhaps they have been. However, the potential afforded by facilities such as the REDCAP and the AF-EWES to support operational testing and tactics development has not been exploited. There is no doubt that imagination and creative thinking can do much to develop the inherent potential of laboratory simulators. However, testers need to recognize that such facilities have an essential role in the EW OT&E process and then resolve to maximize their utility.

SECTION V

INTEGRATED OPERATIONAL TEST AND EVALUATION CONCEPT

Nothing profound so far! EW system testing is tough, we haven't been doing an adequate job, and there are a variety of tools available to be used in the task. Recognizing all that, why don't we just move out and do it right? It isn't that simple, but we can begin to do it better. To do so, however, requires that testers develop a more innovative attitude toward operational testing. It would be nice if we could make "creative thinking" a mandatory qualification for all EW system testers.

Testers, more than anyone else, even when they wouldn't admit it, have long known the limited extent to which the effectiveness of EW systems can be addressed. Perhaps we have caused some of the limitations through our attitudes and approach to testing. If we remain content to constrain testing to a single facility or single mode of testing, then the level of completeness attainable will undoubtedly be inappropriately bounded.

The following approach is suggested as a way to develop specific methodology for EW system OT&E as well as the development and evaluation of tactics for EW systems. The total problem is first broken down into manageable component parts to be examined in the field, in the laboratory, in a model, or in appropriate combinations. Innovative and imaginative analysis and evaluation techniques would then be required to piece together the separate results into a complete assessment of EW system effectiveness.

If such an approach to EW system OT&E is to be effective confidence in this approach and resulting methodology must be established. First, the tester must believe that the approach is the correct way to achieve success and support its continued refinement and development. Second, the tester must be able to articulate to his colleagues and the decision makers the test methodology and the effectiveness test results. The success of a plan, even a very good plan, is largely dependent upon the dedication of those who implement it.

The integrated EW OT&E process is graphically depicted in figure 6. It portrays the use of models, laboratory simulators, and field ranges with extensive information crossflow and feedback.

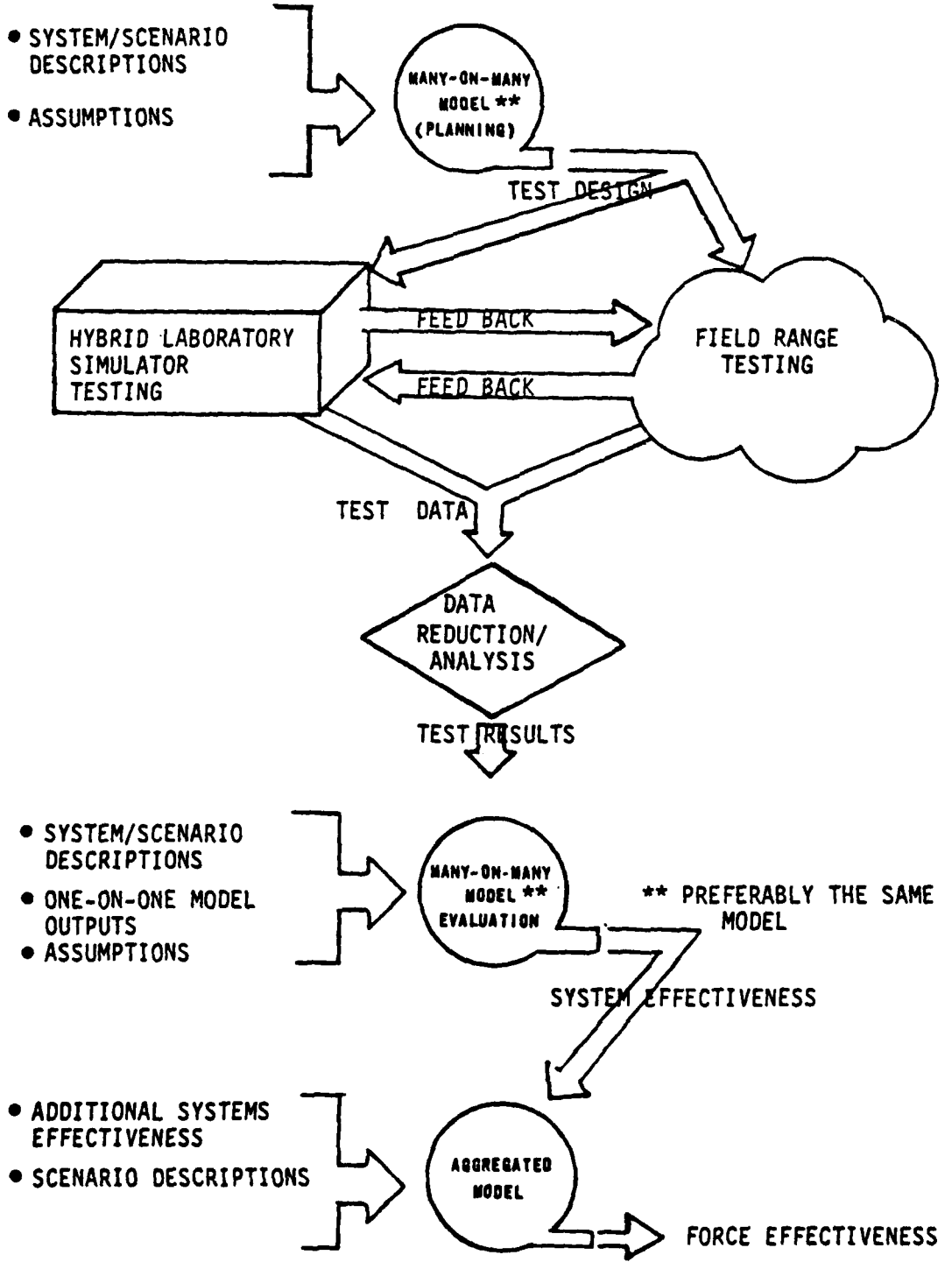


Figure 6. Integrated EW OT&E Approach

Test Planning.

To begin the process, the test planner selects an appropriate model. As described earlier, such a model would describe events in rather rigorous detail. To do so, the model would necessarily have to be sensitive to the specific EW system to be evaluated and accurately model the EW system's characteristics. Obtaining an acceptable model should not be an insurmountable task. Already there exists a proliferation of models for almost any task, and given time and money development of a model for a specific system or purpose can generally be accomplished. The major limitation in using models is obtaining empirical data for correlation; correlation rather than validation seems a more appropriate term. In general correlation as used here would be accomplished by comparing model results with "real life" field testing results from the same scenarios. All variables in a model can be accounted for, however, in field testing all variables are not even known, much less controlled. The important aspect is being able to account for any major differences between "real life" and model results. This accountability is essential to credibility for any subsequent model use. Therefore, from a testing viewpoint the most important consideration for model selection is that inputs be compatible with the types of data obtainable from testing--both on the range and in the hybrid laboratory simulator. This initial modeling effort should be conducted to gain insight into the response of the EW system to input stimuli, a sensitivity analysis. The model should be broad enough in scope to include other systems which interact with the system under test. This includes interactions with both friendly and hostile systems. Models of this scope are frequently referred to as "many-on-many"--less detail than a one-on-one, and much less aggregation than the force effectiveness or campaign models. At this early stage of the process, the model must be used as an experimental tool in the broadest sense, in a parametric manner. Results from this initial effort should not be used to evaluate EW system effectiveness. This early modeling effort should, however, determine a reasonable range of expected system response for various input parameters and assumptions. Thus, the performance of a support

jamming system might be described by the burnthrough range of the screened aircraft as a function of the type of aircraft; the jammer's effective radiated power; and the geometrical relationship between the screened aircraft, the jamming aircraft, and the victim radar. The test planner would be seeking to find those situations which would provide "interesting" test conditions, the nontrivial conditions. As previously stated, the model should at least place the system in a "many-on-many" scenario to determine what interactions with other systems should be accounted for in planning a test.

Just as this early modeling is not intended to determine or evaluate the effectiveness of the EW system, neither is it intended to be a one-time shot. The modeling effort is an iterative process which becomes progressively more refined as the test planner gains knowledge of the EW system's technical characteristics, the environment in which the system must operate, and the ultimate user's intended employment concept. As the process proceeds, the test planner should begin to identify critical data items which must be obtained during actual testing. Early identification of such data items is essential for specifying instrumentation requirements early in the test program. This modeling effort should also afford the test planner an opportunity to evaluate potential measures of merit and to check-out his proposed data reduction and analysis plans. Of course, it should be obvious that tactics developers could also benefit from this early modeling effort by identifying those tactical profiles and formations which appear to be effective.

The basic point to remember is that this early modeling effort should not attempt to evaluate the effectiveness of the EW system or the tactics to be employed and, thereby, supplant the need for testing and evaluation. The model is but one element to be employed in the EW OT&E process. At the initial stage of OT&E, the model is a basic tool to be used in the design of tests which can be conducted at both the laboratory simulator facilities and the field ranges.

Laboratory Simulator Testing.

The role of the laboratory simulator in operational testing is not well defined. The idea is still relatively new, and it is not clear just

how much support such a notion really has. However, from the authors' experiences with the EWJT and, more recently, with the EF-111A test program, we believe facilities such as the REDCAP and the AF-EWES provide great potential to support OT&E of electronic warfare systems. We also believe, just as strongly, that these facilities can play a key role in developing tactics and employment concepts. There are basically two primary areas in which the laboratory facilities can support the overall test and evaluation process: pre-field test and field test complement.

There should be no reluctance to acknowledge that field testing continues to get more and more complex and expensive. Airspace and frequency restrictions, test range scheduling, user training requirements, test resource limitations, funding constraints, fuel allocations, and test reporting schedules are among many factors which strongly influence (limit) the scope of the test program and contribute to the premium placed on available test time. But no matter how careful the planning, uncontrollable problems occur. Aircraft fail to get airborne, radars do not always radiate, instrumentation systems malfunction, and the ever-present Federal Aviation Administration (FAA) directs "cease buzzer."

There are also test design pitfalls which may not be recognized early in the test program. When has there been a perfect match between the type and quantity of data required to adequately address the test objectives and the data which were actually collected and processed for analysis and evaluation? And how often does what seemed to be a reasonably envisioned test condition become trivial and noninteresting when subjected to the realities of an operational scenario? The likelihood of eliminating all of these and other problems associated with EW system testing is low, but their impact can be reduced. The hybrid laboratory man-in-the-loop simulator provides an opportunity to "test the test" before going to the field. The test director can identify sensitive areas which will require special attention in the field, refine instrumentation requirements, revise tactics, and identify the impact of the human threat system operator on the effectiveness of the EW system

under test. In general, the basic result of pre-field testing in the laboratory is that the test plan can be refined and enable more efficient use of the available field range time.

The reader should not be surprised to hear that the existing field ranges are somewhat deficient in their capability to support EW system OT&E. In fact, there are some "gaping holes" on the ranges, and some of them may never be completely filled in. The acquisition time for new threat simulators is no better than that for a new EW system. It is too long! Consequently, the field ranges of today cannot be considered representative of even today's threat environment much less a future threat. Furthermore, the delta which exists cannot be expected to decrease very much at all. Changes in the R&D process could be implemented to significantly shorten management delays in simulator acquisition time, but circuit wiring and metal bending cannot begin without a sound estimate of the threat system's receiver and processing characteristics. Again, these problems will not be totally eliminated, but their impact can be lessened.

The hybrid laboratory man-in-the-loop simulator affords an opportunity to develop a threat environment well in advance of its realization in the field. Many threat system characteristics are software modeled in the laboratory simulator. Hence, a representation of the threat system can be constructed long before its hardware counterpart can be fielded. Additionally, it will possess more inherent flexibility and should not be as expensive to modify or reconfigure if the threat projection changes. This feature is especially beneficial when considering advanced threat systems. There is typically a great deal of speculation and uncertainty surrounding those systems and a concurrent and understandable reluctance to make any commitments to hardware development. Also, it should be recognized that much of the information available on advanced systems is very sensitive, and it may not be appropriate to fabricate such a gadget, haul it to the range, and put it on display (physically or electrically). The laboratory provides the secure features required for work against advanced systems. It also provides the necessary environment in which to evaluate current capabilities against data links and other secure features of the enemy's command, control, and communications structure.

Thus, the laboratory simulator can be regarded as a complement to the field range in two ways: default and design. There are some capabilities which cannot be developed on the range as quickly as required, and should be provided by the laboratory simulator. There may also be some capabilities which should not be developed on the range and, consequently, must be provided by the laboratory simulator.

Keep in mind that we have not advocated use of the laboratory simulator as an alternative to field testing. It is a complement and a supplement. It is efficient to use the simulator before going to the field; it is practical to use the simulator when one cannot go to the field; it is prudent to use the simulator when one should not go to the field.

Field Testing.

Nothing presented so far should be taken as diminishing the necessity for system testing in the field. When electrons are turned loose, interference and incompatibilities usually result. They don't show up in the models or in the laboratory simulator, but they can be nightmares in the field. During EF-111A testing, an ALQ-99E exciter was employed for AF-EWES testing, and it performed well. However, field testing provided a far more realistic assessment of the ALQ-99E as a system consisting of exciters, transmitters, antennas, receivers, etc., all operating simultaneously with other onboard avionics. Interoperability of various weapon systems should be addressed during field testing along with the efficiency of the man/machine interface. While an EW system may be optimized against each threat system in the environment, the aircrew member is actually part of the system and must be able to make it work effectively during the pressures of combat. Aside from the effectiveness issues to which this paper has been limited, there is the major issue of weapon system suitability. This area cannot be adequately assessed in a laboratory environment or a computer model. It can only be adequately addressed under field conditions. It is at least equal to effectiveness as an essential element in evaluating the

military utility of the weapon system. Only in field testing can one truly get the emotional stimulus (sometimes referred to as a "warm feeling") that the system under test actually functions in a realistic environment.

We have indicated that field testing can be accomplished more efficiently by proper use of laboratory simulators beforehand. Notice that figure 6 also depicts the flow of information from the ranges to the laboratory simulators. If there is to be any confidence in the results of testing conducted in the laboratories, then there must be reasonable correlation between those results and the results of testing accomplished on the range under the same test conditions. Hence, it is essential that field test data be correlated with and used in the laboratory simulator whenever possible.

Analysis.

Imaginative test planning and innovative testing are certainly key elements in any successful test and evaluation effort. However, the analysis and evaluation of the data must be recognized as the heart of the test program. Without a sound analysis approach, the collection and assessment of data are haphazard at best, and the test is little more than an exercise. There are some formidable challenges which confront the analyst during this critical phase of the test and evaluation program. Basically, the task is to take the data derived from a collection of relatively small-scale tests, at some less than desired level of realism, and provide a credible assessment of the overall operational effectiveness of the EW system.

One must immediately ask, "What are the measures of an EW system's operational effectiveness?" As discussed earlier, traditional MOEs have included such things as burnthrough range, missile miss distance, delay time, etc. But, are they sufficient? Remember that principal measures of effectiveness must relate to mission accomplishment rather than just system performance. Suppose, for example, that EF-111A desired and/or required level of performance must be rationally determined and effectively articulated as part of the system specifications

provided to the developer. We would hope and expect that such an approach would lead to more operationally meaningful performance specifications for each EW system determined in the context of its contribution to the overall attack effort.

Evaluation.

Since it is unlikely that data from field and hybrid simulation testing will be adequate to directly determine the EW system's operational effectiveness in its intended operating environment, the tester must return to the model(s). As discussed earlier, there are never enough prototypes of the system under test nor enough simulated defense systems to create a realistic threat environment. Feedback from the test data to the model is essential to the successful completion of this modeling effort. Preferably, the same model should be employed that was used earlier in the test design process. The model being used may be one which already existed, or it may have been developed specifically for the particular system under development. A variety of assumptions made during the early modeling effort may now need to be verified. This feedback process, which is most often omitted, is essential for the tester or anyone else to extrapolate test results beyond the narrow conditions of the test. This empirical data feedback is important to the very existence of the model; without it, there is little chance that the model can be validated. Without validation, the model's credibility is in question, and there may be no utility in the tester, or for that matter anyone, using the model.

As stated earlier, the analysis and evaluation efforts are the very heart of the EW system test program. Certainly, the evaluation process tends to be one of the most challenging aspects of the total effort. The problems identified earlier in this paper--limited resources, inadequate test threat environment, evolving system maturation, etc.--contribute substantially to the paucity of quantifiable data available for evaluation. The tester will obviously use any quantitative information obtained from the test effort, but he is most often compelled to rely upon additional sources of data for his final evaluation.

Computer modeling is one of those additional or "soft" sources of data. This phase of the test and evaluation process is where extrapolation is practiced as the tester returns to the many-on-many model. Data derived from a single threat simulator are used to characterize the performance of several such threat systems in the model. Those threat systems, perhaps evaluated singly during field testing, are netted together in the model to represent an air defense system. Of course, if command and control functions were emphasized during testing, then data should also be available for calibrating some of the human responses in the model. On the blue side, scenario changes can also be implemented. Larger attack forces, alternate routes of attack, variations in support concepts, and the introduction of additional support systems may all be possible. The many-on-many model is not necessarily a standalone model. It has, as described earlier, less detail than the one-on-one or system models. Most likely, several different system models may be used to provide inputs to the many-on-many model. The model affords the opportunity to "fight the battle" which was only staged during field and laboratory testing. Through this modeling effort the tester begins to get a feel for the synergisms or disergisms which may or may not exist between various elements of the attack force.

Each person will, of course, view the results of simulation in light of his own understanding of the simulation process. For some, simulation results will never have any utility. For others, the final judgement will be influenced by the quality of the model and the input data. A modeler can usually develop an algorithm which accurately reflects a real-life combat process, but the input data for the model may not be available. For example, the steps involved to accomplish a successful GCI vectored intercept are well understood. However, data such as the controller's capacity to handle multiple target/interceptor pairs may not be known. When structuring field and laboratory tests, the tester must ensure, where possible, that empirical data will be provided to narrow the range of uncertainty of the model's inputs. The type and proportion of input data which is based upon empirical test data rather than scientific and technical assumptions is critical to the credibility and usability of the results. When results are very sensitive to input data,

and the input is based primarily on assumptions, then the caveats which accompany the assumptions are what most often cause the simulation results to be regarded as soft.

Another source of soft data is the tester. His intuition, judgement, and experience contribute to his subjective assessment of an event, situation, or occurrence. Ironically, while this form of data may be considered soft, it has often been the major source of information used in the decision process. The tester has the opportunity to observe the EW system through various stages of growth to a level of maturity which he recognizes as an operationally effective system. He recognizes the deficiencies in the EW system, but more importantly, he understands the operational impact of those deficiencies and whether or not effective workaround procedures are required and can be developed. Often times, the tester plays a key role in refining or modifying the proposed operational employment concept based upon increased knowledge and understanding of the system's performance and capabilities. The tester also tends to be the first to observe capabilities and effects which may not have been anticipated. Consider the EF-111A's role in close air support (CAS) operations. During IOT&E, the accepted MOE had been a specified reduction in SAM firings against A-10 aircraft. The measured reduction failed to reach the threshold evaluation criteria, and the EF-111A's performance in the CAS role could have been rated deficient. However, the distribution of SAM engagements had been significantly altered so that the A-10's probability of successful attack was increased. Also, the radiation patterns of the threat radars were noticeably changed in a manner which would favor Wild Weasel and PLSS operations. When these factors were combined with the modest SAM firing reduction, the EF-111A's performance was considered satisfactory. This assessment was subjective and was the best judgement of the tester. Perhaps it is a soft source of data only to those who fail to recognize its ingredients. The professional judgement of the EW system tester tends to be one of the bright spots in the test and evaluation process, and it certainly should not be discouraged or undermined.

Force Effectiveness.

The final phase of the proposed integrated OT&E methodology for EW systems is an area which surely interests the tester, but he should not be responsible for it. The level of extrapolation attempted with the aggregated model transcends the many-on-many efforts.

Recall that the aggregated model tends to generalize the specific effects of both red and blue systems while accounting for their contribution to some larger event-oriented process. This modeling effort tends to address force structure issues and to estimate the marginal utility and/or cost effectiveness of the proposed EW system. This task is clearly beyond the charter of the tester. The same points which were made in favor of the tester's subjective assessment capability are detractors from his ability to perform this modeling effort. The tester understands the EW system under evaluation at least as well as anyone. He knows what the system can and cannot do and how it performs in specific situations. However, it is not likely that he possesses similar knowledge and understanding of other systems which would be considered in a thorough force structure or cost effectiveness analysis. Such analyses are the kinds of tasks more appropriately addressed by agencies such as Air Force Studies and Analysis (AF/SA). Hence, a close working relationship should be maintained between AF/SA and the operational tester. This liaison should begin early in the OT&E program and continue through all phases of the process portrayed in figure 5 and described in this paper.

The integrated methodology for EW system OT&E which has been proposed in this paper can be summarized very briefly:

- Initial modeling phase for sensitivity analysis and test planning.
- Active test phases at hybrid laboratory simulators and field range facilities.
- Test data reduction and analysis.
- Post-test modeling phase repeating the first step using test data for extrapolation.
- Force effectiveness modeling and analysis phase to determine the incremental contribution of the new system to total force effectiveness.

Demonstrating Concept Feasibility.

Sound test design, planning, execution, and evaluation are imperative for credible EW OT&E. Those tasked with such responsibilities must actively seek methods of using the capabilities of analytical models, laboratory simulators, and field ranges to their fullest. The best example to date of an innovative and creative test and evaluation process for evolving electronic warfare systems is the EF-111A TJS test and evaluation program. During that program, planning, testing, and evaluation were accomplished with two computer simulation models, two laboratory simulator facilities, and two field ranges. Each element of the effort was designed primarily to address a specific portion of the overall test requirement.

Test planning essentially began with the SABER COUNTER ECHO study effort conducted by AF/SA in 1973 to support the EF-111A DSARC I. The major analytical tool employed during that study effort was The Air Combat Operations Simulation (TACOS) computer model, a many-on-many simulation. Included in the inputs were data developed at the AF-EWES using the one-on-one hybrid simulators. Attack aircraft employment, EF-111A support, and threat system deployments were representative of those expected during a central European conflict between US and Soviet Bloc forces. Data from REDCAP was also used in the SABER COUNTER ECHO study. The REDCAP was again used during the DT&E/IOT&E to assess EF-111A receiver and processor performance in a dense emitter environment. The facility was also used to pretest the flight test profiles which were to be flown during testing at the Nellis AFB Test Ranges. The TACOS model had been used to develop candidate flight test profiles and to generate terrain masking events for use in the simulator. The subsequent REDCAP effort provided needed insight into the EF-111A's capability to screen escorted aircraft and aided in the refinement of the flight test design. Flight testing on the Eglin AFB Range provided aircraft performance results and an assessment of the jamming capability against individual threat radar systems. Flight test data collected at the Nellis AFB Test Ranges were used to evaluate the EF-111A's capability to penetrate an enemy

integrated air defense system and its impact on the command and control of SAM, AAA, and airborne intercept (AI) weapon systems. The AF-EWES provided an enemy Combined Arms Army environment which was not available in the field and permitted an assessment of the effectiveness of support jamming during close air support and battlefield interdiction operations. Once again, the TACOS model was employed as a tool for developing attack profiles and terrain masking events for use in the AF-EWES. Following completion of field and laboratory simulator testing, the Tactical Air Defense Battle Model (TADBM), a many-on-many simulation, was employed by AF/SA as a tool for extrapolation and evaluation before the DSARC III.

The process followed during EF-111A testing nearly coincides with the proposed concept. The most noticeable departure is the change in computer model for post-test evaluation. Also, the total process was not as smooth as it may appear from the above description, nor was it entirely pre-planned. Much of the process evolved as the test program progressed. It is important to recognize that no single test element nor even a single type of test capability could have permitted such a comprehensive evaluation of the EF-111A's effectiveness. Each element provided a unique capability which was required and effectively used to achieve the overall test and evaluation objective. During the EF-111A program reviews, OSD personnel repeatedly stated that the operational effectiveness evaluation of the EF-111A was the most comprehensive OT&E to date of any EW system. A final note of caution, the existing test facilities are still not completely adequate and require continued upgrade and enhancement even though substantial investments were made during the EF-111A test and evaluation program.

So far, this paper has been limted to a philosophical discussion of EW system OT&E. We have described an approach for using analytical models with hybrid laboratory simulators and field testing. It is an approach which we believe can improve both the quality and credibility of EW OT&E. We have also indicated that this approach is not and should not be restricted to testing. The concept is certainly applicable to the tactics development business. In fact, it is difficult to envision any viable process for developing a comprehensive defense suppression concept which would not parallel the approach presented in this paper.

It is not practical to bring together for an extended time a large number of systems such as EF-111A, F-4G, PLSS, Pave Mover, etc., to try out a large number of concepts to find out how best to use a system in a cooperative manner. On the other hand it does seem practical to represent such systems in hybrid and digital simulations to develop and determine feasible concepts. Those few concepts which do show promise can then be evaluated during field testing.

The concept proposed in this paper for test and evaluation of EW systems requires adequate test facilities to permit successful application of the approach. Unfortunately, the current capabilities of existing test facilities--both field ranges and hybrid laboratory simulators--do not satisfy that requirement. To accommodate the EF-111A test and evaluation program, extensive upgrades and improvements were implemented at the field ranges and at both REDCAP and AF-EWES, the hybrid laboratory simulator facilities. In spite of those efforts, the facilities still provide only a minimal capability to support operational testing of EW systems, and further improvements are required. The following section will provide a brief overview of the test environment we believe is required for EW system OT&E.

SECTION VI

REQUIRED THREAT ENVIRONMENTS

In general, as stated earlier, the test environment required is that which provides a credible representation of the expected operational environment. Obviously, an attainable test environment will be significantly less complex than a real combat environment. The question to be answered is how complex a test environment must be for sufficiency. This issue of sufficiency must ultimately be addressed on a case-by-case basis. However, the problem of developing adequate test facilities should not be approached on a case-by-case basis. Overall goals should be established and a roadmap approach used to develop test facilities. Since the basic test facilities are required by research and development agencies and by the operational commands for both tactics development and training, the overall plan for their development must be a coordinated Air Force effort.

Defense suppression EW systems counter airborne, as well as fixed and mobile ground threat systems, although any single system may not necessarily operate against all types of threats at once. Therefore, test facilities must provide the required threat systems, proper surveillance and acquisition systems, the correct command and control structure, and valid operating procedures. Of course, shipborne systems should be included for certain scenarios. However, for brevity, scenarios for shipborne threats will not be specifically discussed. They would be treated much like the ground-based systems.

Threat Environments.

The airborne intercept test threat environment needs both ground-based and airborne elements. A network of GCI radars is the basic element of the ground environment. It may also be appropriate to consider an airborne controlled intercept (ACI) capability for this threat environment. The remaining airborne elements would naturally be the fighter aircraft. For the range, the ground components of this

threat environment can be provided by hardware simulators, but the airborne elements will most likely need to be represented by surrogates. Surrogate systems will be discussed in more detail in a subsequent section. The hybrid laboratory facility should be capable of modeling both the air and ground components of the threat environment. In addition to the aircraft and radar elements of the threat environments, it is necessary to tie them together. Both voice and digital data link communication systems should be available between interceptors and weapons' controllers. It is imperative that the simulated threat systems deployed in the threat environment be employed by skilled personnel using valid operating procedures and tactical doctrine. Finally, the threat environment should possess adequate configuration flexibility to account for various threat scenarios. For example, the tactics, procedures, and equipment employed by the PVO STRANY against a manned strategic bomber may be significantly different than those used by a Tactical Air Army against multiple fighters in the Central Region. The threat environment, to assure testing sufficiency, must be adaptable to the specific weapon system and tactics to be evaluated.

The "fixed" ground threat environment is predominantly comprised of nonmobile SAM and AAA defense systems. It may not be entirely appropriate to refer to such an environment as fixed; therefore, the word is used loosely. This type of environment has sometimes been referred to as "strategic," probably because it is most representative of the PVO defense structure. The threat environment for testing should provide a representation of the defense structure about reasonably fixed target complexes. These would tend to include airfields, command centers, etc. The threat environment should provide the basic elements associated with the integrated air defense structure of a Soviet Air Defense Region. A radar early warning system is required with both frequency and PRF diversity as well as overlapping radar coverage in both range and altitude. Individual radars should be netted together with both voice and digital data link to, as a minimum, a semiautomated command and control system. As indicated before, the basic terminal defense systems required for the threat environment are nonmobile SAM and AAA systems. Mobile systems need not be excluded, but systems such as the SA-2, SA-3, and SA-5 SAMs along

with AAA should provide the primary defense. Additional threat systems which should be considered in the threat environment are those active and passive EW systems which are deployed with the lethal defense elements. Again, it is imperative that the threat systems deployed in the threat environment be operated by skilled personnel using valid operating procedures and tactical doctrine. And, the threat environment must be sufficiently flexible to provide valid representations of various scenarios. Hence, it must also be capable of rapid adaptation to the changing threat environment.

The mobile ground threat environment should provide a reasonable representation of a Soviet Combined Arms Army; occasionally referred to as a "tactical" environment. The air defense structure should include early warning/surveillance units, as well as the mobile SAM and AAA systems which are associated with the tank and motorized rifle forces. Command and control requirements for this threat environment are probably more complex than for the other required environments due to the mobile nature of the various threat systems. However, the distinctive command and control features associated with the SA-4, SA-6, SA-8, and any other SAM systems, which may be deployed with the field army, should be adequately represented in the threat environment. Their interfaces, if any, with each other or with other elements of the total defense network should also be provided. Additionally, the active and passive EW assets organic to the field army should be included in the threat environment. As with the other two required environments, airborne intercept and fixed ground, it is imperative that the simulated threat systems deployed in the threat environment be employed by skilled personnel using valid operating procedures and tactical doctrine. This threat environment must also be readily adaptable to the rapidly changing threat.

It should not be inferred that the three basic types of threat environments which have been identified must be treated as separate and distinct. The requirement is to provide the basic representative threat environments in which electronic warfare systems can be evaluated. Two or more of the basic environments could be provided by a single facility, or a combined environment could be represented, in the

field, by multiple adjacent facilities. It is important to recognize the types of threat environments in which the EW systems are intended to operate, and to provide adequate facilities for effectiveness evaluations.

It is reasonable to request a definition of "adequate facility." What is required has been presented in a rather generalized manner. Just how much is required? How much of the actual threat environment must be characterized in the test facility for it to be adequate? A tough question! We don't pretend to have THE answer, but we do have some suggestions to be used for guidance.

There appear to be two basic aspects to the "size" of the threat environment, which we call horizontal and vertical. As we define it, horizontal refers to the types and numbers of threat systems; the density of the environment. Vertical refers to the command echelons or levels of decision making within the defense structure. Horizontal is the feature most thought of when considering how much; vertical is certainly at least as important. Neither facet can be slighted in the development of a threat environment. It is important that each specific threat system be represented in the threat environment. It is important that, to the extent possible, threat simulators be deployed in multiples to provide an environment in which to assess receiver/processor capabilities, especially power managed systems. All threat simulators need not have the same level of sophistication. This is explained in more detail later. It is also important that each element within the decision making structure be represented. Further, it is important that at each echelon where decisions are being made, there be at least two subordinate elements in the system. The operator tasked with making a decision must have some alternatives from which to choose.

When considering "how much," one should also be concerned with developing redundant capabilities. It can be bad or good depending on the nature of the redundancy. For example, it would not appear to be very efficient to maintain two field ranges which both provide the same capabilities. On the other hand, it would be appropriate to develop similar capabilities at both a field range and a hybrid laboratory facility. In fact, such parallel development is necessary to permit effective

pre-field evaluation in the laboratory as proposed in this paper. Hence, each of the basic test threat environments described above should be developed in a hybrid laboratory facility and, to the maximum extent possible, at a field range facility.

Three basic types of required test threat environments have been briefly described. One should also understand what such an environment must consist of to support EW system OT&E. The basic ingredients in any good test threat environment are the threat system simulators, the threat system operation, the instrumentation system, and the data management system.

Threat System Simulators.

Threat simulators have been categorized and defined according to their capability to represent the intended threat system (see figure 7). Four basic categories have been established and defined to represent the various levels of radar simulators. The definitions could just as well apply to nonradar systems which operate within the electromagnetic spectrum.

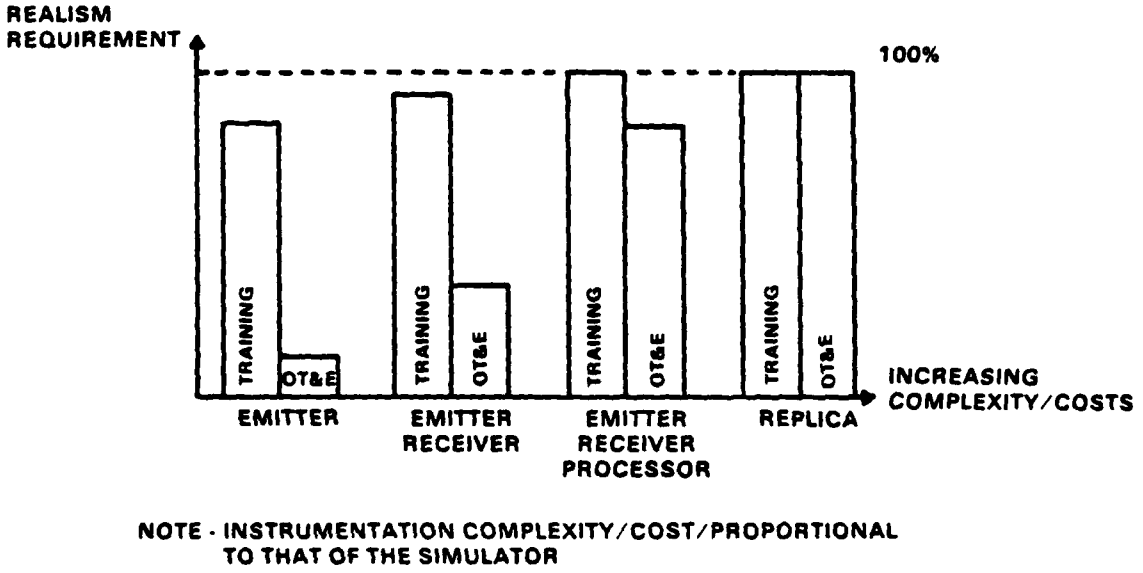


Figure 7. Threat Simulator Usability

The emitter simulates some of the threat system's emitted characteristics, but it has no receiver. The emitter is the least sophisticated and the least expensive threat simulator. It can satisfy many of the threat realism requirements for training, but it has only limited utility in EW OT&E. That utility is increasing with the continuing development of power managed ECM systems. Dense threat emitter environments are required to properly assess the EW system's capability to process large quantities of threat signal information. Emitters are a cost effective method of creating RF density in a test threat environment.

The emitter-receiver also simulates the signals emitted by the threat system. It also provides a representation of the threat system's receiver capability, although it may be no more than a spectrum analyzer. Its utility for both training and OT&E is greater than the emitter. While its receiver may not be suitable for evaluating ECM effectiveness, it at least permits verification of the EW system's response to the simulated threat system. Consider the COMPASS TIE system as an example. Using emitters, a dense RF environment could be provided at relatively low cost to stimulate the radar warning receiver in the aircraft. A few emitter-receivers could be deployed within that environment to monitor the response of the aircraft's jamming system (e.g. frequency, bandwidth, relative power, etc.). The effectiveness of the jamming response could be determined using a more sophisticated simulator, or it might be estimated from calculations using data recorded at the emitter-receiver.

The emitter-receiver-processor is an electrical representation of the threat system. It provides the best estimate of the threat system's receiver and signal processing characteristics. It represents a sufficient level of simulation for valid EW OT&E in nearly all cases.

The replica is a functional representation and look-alike of the threat system. Mobility may not be completely duplicated. Replica simulators are generally developed based upon exploitation data and are the best, the most realistic, and the most desirable level of threat simulation for EW OT&E. It is also the most expensive and difficult to achieve. While the higher level simulators such as emitter-receiver-processors and replicas can satisfy training requirements, their marginal utility in such a role decreases because of the high cost.

The preceding described the four basic categories of threat simulators. However, for some the list would not seem to be complete. There are no categories which define or describe systems employed to represent or simulate advanced capability threats nor those threats for which we possess no simulator. We would propose that, in addition to the four simulator categories already described, two further simulator categories be considered: adaptive and surrogate.

The adaptive simulator would provide a representation of the anticipated or postulated capabilities of advanced threat systems. Such a simulator would not be developed to provide the specific characteristics of any particular threat system. The adaptive simulator would most likely be used primarily for development testing and would probably have limited usability for EW OT&E. For testing based on sensitive information on advanced state of the art systems, the adaptive simulator would probably have very limited use in the field. It should be developed primarily for use in the hybrid laboratory facility where security can be maintained, and the flexibility and adaptability afforded by the laboratory can be used effectively.

The surrogate simulator is a "friendly" system which is employed to provide a representation of a known or postulated threat system. The surrogate is used when no conventional category threat simulator exists, and perhaps as a gap filler to increase threat density in the test environment. We have been using surrogates for years; it is time they were recognized as a simulator category.

It should also be recognized that the complexity and cost of threat simulator instrumentation is proportional to that of the simulators. As the level of threat simulator sophistication increases, there are greater requirements for information to be derived from the simulator. Hence, the level of required instrumentation is also greater, and it is a factor which must be accounted for as an integral part of simulator development. The collection of data is an essential and distinctive characteristic of the test and evaluation process. Without data, a test is no more than an exercise. At the same time, feedback of information from the threat environment is also required by those involved with training and tactics development. Without it, the success of their efforts will largely be speculation.

Simulator Validation.

There is an additional aspect of the threat simulator development program which is critical to effective EW OT&E -- validation. The extent to which the threat simulator electronically represents the actual threat system must be determined and documented. Effective simulator validation can be described as a three-phase process: design, performance, and operational.

Threat simulator development begins when the Air Force provides an intelligence data input package (IDIP) to the designated simulator builder. The IDIP describes the threat system's characteristics in sufficient detail to permit development of a representation of the threat. The builder, using the IDIP, formulates a design for the threat simulator. The first phase of the validation process occurs at this point. It must be determined that the simulator, if constructed according to the design, will provide a system with the characteristics and parameters described in the IDIP.

Once the design validation has been completed, the builder proceeds with construction of the simulator. When construction is complete, the capability of the simulator to perform according to the threat projection must be determined. This phase of the validation process is considerably more difficult than the design validation. For various technological reasons, the simulator will probably not be a duplicate of the threat. Depending on the degree of divergence between the threat and the simulator, the magnitude of the differences may or may not be an important factor. Thus, it is essential that the impact of those differences be documented and made available to the users of the simulator.

The final step in the validation process is no less important for EW OT&E, but it is the most neglected. Once a threat simulator has been developed and accepted, it must be deployed and employed in accordance with the best available intelligence estimate of the threat system's operation. Unfortunately, that estimate has not always been provided,

and threat simulator operators have had to devise their own operating procedures and employment concepts.

There is an additional problem which must be recognized as occurring even after a validation process has been completed. It is characterized by the insidious deterioration of the validity of fielded threat simulators. Once developed, fielded, and operated, threat simulators must be maintained. It is essential that threat simulators be continuously monitored for acceptable performance; the operational validation phase of the process must be continued throughout the life of the simulator.

Recognizing the problems confronting the intelligence community helps one understand the dilemmas inherent in the simulator development and validation process. Quite understandably, the initial IDIP provided to the simulator developer is usually incomplete. The exigencies of the situation demand some representation of the threat. A "get started now and update later" philosophy makes the validation process difficult at best. In the past, it has frequently produced unacceptable threat simulators because the updates were delivered to the developer at about the time the simulator was being delivered.

Even when the simulator is developed from a good IDIP, the tester himself may preempt the validation process. The time required to produce a threat simulator fuels the anxiety of the EW system developer and tester. Ironic as it may seem, the eagerness to test against the new simulator has often outweighed the desire to have a validated simulator. That should be less of a problem in the future with hardware simulators now being developed for the field ranges. Simulator validation is being planned and funded as part of the simulator development program.

Remember, however, that the field range is only one asset available for EW OT&E. The validation process must also be applied to the hybrid laboratory simulators and the analytical models. Current hybrid laboratory simulator validation procedures are incomplete; model validation is virtually nonexistent.

Effective, thorough, and continuous threat simulator validation is an absolute must. Without it, the tester will probably expend more effort defending the credibility of test resources than describing the new EW system's effectiveness. Without validation, even the tester will have doubts about the validity of test results.

Threat System Operation.

Threat simulators are certainly necessary elements of the test threat environment, but in the OT&E business, the man-in-the-loop is a critical factor as EW is directed against both hardware and operators. At least as important as the development of hardware for the test facilities is the validity of the procedures employed by those who operate the equipment. We have repeatedly stated that it is imperative that the simulated threat systems deployed in the threat environment be employed by skilled personnel using valid operating procedures and tactical doctrine. Unfortunately, that is one of the "gaping holes" referred to early in this paper. Neither the skilled operators nor the valid procedures are currently available at the existing test facilities. The "owners" of the facilities do not provide to the tester documentation which validates their procedures. Of course, the operators generally know how the simulator functions and how to use it, but that is not sufficient to guarantee correct employment. In the past, extensive efforts to develop operating procedures and train simulator operators have been attempted by OT&E test teams. Those efforts have not been totally successful.

During the EWJT, test team personnel researched available intelligence documents and eventually developed a comprehensive doctrine for red force operations. An extensive training program was established to teach both threat simulator operators and observers/data collectors the fundamentals of integrated air defense system operations. During the EF-111A IOT&E, test team personnel again prepared a rather comprehensive operating doctrine for red force operations. A training program was established to orient the simulator operators to the procedures. There were many discouraging similarities between these two test programs:

- o There were no existing operating procedures for the threat system operators.
- o The simulated red force doctrine was developed by members of the test team.
- o The intelligence community did not actively participate in the red doctrine development.
- o The red doctrine was not approved or validated by the intelligence community.
- o The training program was not adequate to overcome established procedures and operator tendencies.

Both EWJT and EF-111A test team personnel sought assistance and advice from various elements of the intelligence community. The support was not adequate and the test teams tackled the job themselves. For a tester, it is difficult to develop a red doctrine; even more difficult to get it validated, blessed, or approved. The tester has generally settled for a rather innocuous pronouncement like, "I have no information to contradict any of your proposed doctrine." That has had to suffice, adequate or not. This process has generally produced acceptable operating procedures even though it is not the preferred method of doing business. Success must be attributed to the experience, background, and dedication of individual test team members. This approach provokes challenges against the credibility of the test program as the test methodology becomes the focal point for criticism.

It would certainly help if we had a Red Force. A cadre of personnel should be selected to operate the simulated defense threat environment. That means decision makers as well as simulator operators. The air defense system must be operated according to a validated doctrine provided by the intelligence community. Red force personnel must receive a comprehensive indoctrination and training program. It is necessary that they perform according to the doctrine, but they must also know and understand the doctrine. They should, as much as possible, think red!

Instrumentation System.

The threat simulator is certainly regarded as the cornerstone of the threat environment. However, as indicated earlier, without data a well intended test is no more than an exercise. There are three basic categories of information which must be provided as a function of time during an EW test effort: the position of each element or participant of the simulated battle, the status of each emitter in the scenario, and the actions of each test participant.

Player position within the test environment is provided by time-space-position information (TSPI) systems. The accuracy of the information provided is dependent upon the type of TSPI system employed. In general, there are two categories of TSPI required for EW testing: area and precision. Area coverage is necessary to provide information on the locations of relatively large numbers of aircraft which may be anywhere within the test environment. The accuracy requirements for such data depend upon the test objective, but in general, the data should permit identification of individual aircraft within multiple aircraft formations. An argument for less precision could be offered if the only objective were to determine initial detection range at an early warning radar, and the entire aircraft formation was expected to be within the radar's resolution cell. Individual aircraft position would then not be required. However, detection information alone would provide little insight into the EW system's contribution to attack force survivability. The tester must, as a minimum, determine an estimate of the threat system's capability to engage the attack aircraft. For any simulated SAM, AAA, or AI engagement, the tester must be able to identify the intended victim. Arguments have often been put forth that this requirement is not necessary to determine "what" happened during an OT&E. However, the tester has failed in his duties if he is not also prepared to describe "why" events occurred as they did. An example to illustrate this point would probably be helpful.

A major joint service test was conducted several years ago to determine the relative effectiveness of various EW techniques and concepts. Aircraft penetrated the simulated threat environment, attacked

their assigned targets, and withdrew from the area. One of the test conditions called for the attack aircraft to employ only their self-protection ECM systems for EW support. Another condition provided only corridor chaff as the EW support for the penetrating aircraft. The prescribed MOE was the rate of attack aircraft engagement by the simulated SAM systems. There was no apparent significant difference in the SAM engagement rates obtained from the two test conditions, and it was erroneously concluded (by some) that the chaff was no more effective than the existing on-board jamming system. However, closer inspection of the data indicated that one aircraft in the formation received most of the simulated SAM firings. Video recordings of the threat radar scopes indicated that the victim aircraft could not maintain formation and stay in the chaff corridor. Tactics rather than ineffective chaff was the real problem, but it would not have been detected without adequate data.

Precision TSPI is required when threat system tracking errors are to be measured and used for estimating simulated missile or projectile miss distance. The TSPI system's accuracy should be, as a minimum, sufficient to determine whether or not the missile miss distance is less than its warhead's lethal radius or to determine whether a projectile firing is a hit or a miss. This form of tracking is generally constrained to a one-on-one configuration; only a single aircraft tracked by each TSPI radar.

Generally stated, the TSPI requirement is for a system which can provide accurate location information on individual aircraft within multiple aircraft formations, operating over a relatively large geographic area, and at low altitudes. Not an easy order to fill! Some multilateration systems have recently been introduced, but they have limited range and do not provide the accuracies required for missile miss distance. They also have severe problems tracking aircraft operating at low altitudes and generally provide large altitude errors. The NAVSTAR Global Positioning System (GPS) appears to offer an acceptable solution to the problem, but it is still several years away. Since EW OT&E cannot wait until then, some interim solution is required. It seems reasonable to suggest that existing area and precision systems

could be integrated through software to provide an adequate TSPI capability. A phased array radar system could be employed to establish individual aircraft tracks and provide the desired aircraft position throughout the test environment. Threat simulator tracking data could be compared with the area TSPI data, and precision tracking radars could then be slaved to the simulator during the engagement to provide reference position data on the intended victim aircraft. Such an arrangement would provide aircraft tracking to satisfy area and range safety requirements and would also provide precision tracking when necessary. Since aircraft position information is an input parameter for hybrid laboratory testing, the TSPI problems encountered on the range will not exist in the simulator.

The principal components in any EW test are the systems which emit RF energy and those which receive it. It is essential that the performance of these systems during the test be known by the tester. It is not uncommon for a radar warning receiver to appear deficient for not identifying known threats only to later learn that the radar was not radiating or was operating incorrectly. It has also been our experience to find that ineffective jamming at the radar can often be attributed to malfunctioning or incorrectly programmed ECM equipment. Spectrum monitoring systems are required as part of the test facility's total instrumentation capability. They must provide the capability to monitor and record, as a minimum, the operating frequencies of all ground and airborne emitters participating in the test--jammers, radars, radios, data links, etc. Of course, it would also be helpful if these systems could provide additional data such as PRF, pulse width, and relative power--especially a received jamming signal strength at the victim radar. In any EW test, there is an RF background which is generally not well known. It is provided by systems which may or may not be directly associated with the test effort, but they exist within the area. Television, TACAN, FAA radar, marine radio, etc. contribute to the RF background and should also be monitored and recorded by the instrumentation system. To correctly assess the effectiveness of the EW system under test, the OT&E tester must know the environment in which the system was operated.

The final element of the instrumentation system provides the capability to determine the manner in which equipments were operated. It is the capability to monitor and record switch actions and events--especially decision making events. This form of data is generally referred to as diagnostic. It affords the tester the opportunity to reconstruct the event which occurred during the test and be better able to determine why the event occurred as it did. An aircraft's jamming may well be ineffective due to the radar operator's use of a certain ECCM fix, or the aircraft's RWR may fail to detect the SAM launch because of the attitude of the aircraft at the time. As stated earlier, the tester's task is not complete if he has not determined the "why" as well as the "what;" diagnostic data are required to accomplish that task.

Data Management System.

If the analysis and evaluation effort can be considered the heart of the OT&E process, then the data management system can be no less important to the test facility's support capability. In fact, without data there is no test. Or, more appropriately, without usable data there is no test. Testers can undoubtedly recall countless boxes, rooms, and computer tapes filled with data waiting to be interpreted and formatted so it could be used. That certainly delays the completion of the test report, but there is a much more insidious aspect to the absence of timely data. Test control may be sacrificed without accurate and timely data. In general, the tester has three needs which must be satisfied by the test facility's data management system: real-time, quick-look, and post-trial.

The tester must be aware of "what's happening" when "it's happening." That doesn't mean he needs to know how electrons are interacting during an EW test. But he should know that aircraft are penetrating along the designed flight paths, that radars are functioning properly and being operated according to specified doctrine, and that instrumentation systems are working and producing data. Real-time data are essential for test control. If the test mission is not going as planned, and is not going to produce usable data, it may as well be terminated. Without real-time data, the tester may find out the mission

was a bust, but it could be hours, days, or even weeks before he does. During the EWJT, threat radar simulators occasionally received jamming from passing B-52 aircraft regarding the radars as targets of opportunity. The jamming was unplanned, unwanted, and, more importantly, unknown to the test team until after testing had been completed. The missions were interesting but of no value to the test effort. Without real-time data, the tester relinquishes control of the test to the fortunes of chance.

Very early in this document, we indicated that EW OT&E has been constrained by an incomplete knowledge of how a system will work and how it should be employed. Frequently the tester can learn only through trial and error just what he should be testing for. The tester must have reliable data which permit him to assess the worth of the test mission prior to the next scheduled mission--quick-look data. If the reasonably envisioned test condition becomes trivial and noninteresting when subjected to the realities of an operational scenario, it is pointless to replicate the condition. Who needs high confidence in a worthless effort! On the other hand, when a valid test condition trial is spoiled for some unforeseen reason, it is worthwhile repeating the test mission. There is another reason for having quick-look data. At the end of each mission, at least a superficial data reduction and analysis effort should be conducted. If the tester waits until the test is over to try his planned data reduction and analysis system, he may be in for a shock. Horror stories abound. Often new software programs are developed for a test. Information is stored on a magnetic tape. Sometimes the collection system "hiccups." Timing gets off. It may be necessary to rely on manually recorded data to decipher computer recorded data. Sometimes the requested accuracy of measurements is inadequate. Consider the system which provides radar pointing data as a pen trace on a strip chart where a distance of approximately 1/16-inch represents a radar antenna angular difference of 15 degrees. Just try to use it to determine which aircraft within a formation was engaged. Anyone who has been there could undoubtedly recount many seemingly unbelievable "data tales."

The basic point is that the tester must receive timely and accurate data in a usable format--usable to the tester. That means test facilities need sufficient flexibility within their data management systems to satisfy the individual requirements of various users. Testers have wanted this flexibility for several years, but they probably couldn't justify it because they really didn't know what they wanted. The "vacuum cleaner approach" was the rule rather than the exception; take everything you can get your hands on and figure out what you can really use after studying it. That approach can generally be attributed to inadequate planning. The concept presented in this paper can help improve the planning process and provide more specific and reasonable data requirements. The test facility is then obligated to respond to and satisfy those requirements.

Current Initiatives.

At the beginning of this section, it was stated that the current capabilities of existing test facilities, both field ranges and hybrid laboratory simulators, need to be improved to facilitate successful application of the OT&E approach presented in this paper. They do not provide the level of realism required for current and future EW system testing, their instrumentation systems are inadequate, and their data management capabilities are generally not responsive to the user. As was discussed earlier there is a proliferation of all kind of models and no restrictions on developing new models. However, while obtaining an appropriate model can be accomplished, obtaining credibility for model results is not so easily achieved. Where do we go from here? The picture may be bleak, but certainly isn't hopeless.

There are several initiatives, some more successful than others, which are intended to improve the testing environment. Field ranges are now being developed according to plans provided by a range improvement working group. There is no similar working group controlling the current or future development for the hybrid laboratory simulators. The Assistant Chief of Staff for Intelligence is formulating an aggressive range simulator validation program. Aeronautical System Divisions (ASD) is requesting additional funding for validation of the

simulators at AFEWES. There is a lot of interest in improving the hybrid simulators but current initiatives are basically uncoordinated. There is no master plan for coordinating and directing the individual efforts to achieve some larger goal. Because of the proliferation of models and the ease of developing new models it may be impractical for any one agency or group of agencies to have responsibility for model control. It is incumbent upon the agency using a model to select a model which already has credibility or conduct specific correlation analysis to address model credibility before using it. Organizations such as AFTEC have unique capabilities through testing to develop credibility for models which it chooses to use. AFTEC and AF/SA are working together to use, where possible, the same models. The ASD has taken on the task for maintenance of a family of SAM/AAA engagement models (TAC Zinger) which have been developed by AF/SA. In general, the current initiative for field range improvement seems about right, model problems must ultimately be solved by each agency, but initiatives for improvement of hybrid laboratory simulators must be considered inadequate.

The concept presented in this paper must be regarded as an integrated use of field ranges hybrid laboratory simulators, and analytical models. Consequently, failing in any one area seriously degrades the overall utility of the approach. As was discussed earlier, improvements for field ranges based on a plan are now starting to take place and problems with analytical models are manageable. It is in the area of hybrid laboratory simulators that management attention must be focused. It is apparent that there is no master plan in which all individual efforts are channeled to achieve some overall goal. A master plan should be developed by all the users of the facilities. The authors have reviewed the facilities and have specific recommendations for their improvement. While the recommendations were made from an OT&E viewpoint, they should be very close to satisfying the needs of all users. To illustrate the types of improvements being referred to, a discussion of the AFEWES facility follows. A similar type of review could be conducted for REDCAP.

AF-EWES.

The AF-EWES has continued to evolve since its inception in 1958. However, the development has been largely directed in response to individual users rather than being based upon a well structured plan with specific goals. Simulations of enemy threat systems have been developed with sufficient detail to permit the evaluation of specific ECM techniques against those systems. Evaluations have primarily been conducted on self-protection systems with from one to four target aircraft operating against a single SAM or AAA system.

During the EF-111A IOT&E, which was conducted in 1978, it was necessary to determine the capability of the EF-111A/ALQ-99E to provide effective support jamming for attack aircraft conducting close air support and battlefield interdiction operations. The threat systems to be encountered during such operations were not available on the test range, and AFTEC opted to utilize the AF-EWES for this phase of the overall test effort. However, extensive modifications were required to provide a capability to simultaneously operate three radar simulations and develop the appropriate command, control, and communications structure between them. The simulator's target capacity was also expanded from four aircraft to forty.

The EF-111A/ALQ-99E jamming test was a first attempt to operate the AF-EWES radars in a netted manner. The test demonstrated the extensive software development effort required to integrate multiple radars and computers. The test proved to be successful in providing a useful (though admittedly not complete) assessment of the EF-111A's support jamming capabilities against the postulated threat deployment of a Combined Arms Army. However, it also highlighted several weaknesses/deficiencies which require strengthening/resolution as part of a continuing development and enhancement program.

An AF-EWES upgrade/enhancement program should be designed to develop the capability to provide a threat environment which is representative in number and type of the air defense structure associated with a Soviet Combined Arms Army. Since there is no one threat deployment that will satisfy all users, the facility should be capable of

rapid adaptation to changing threat scenarios. Finally an upgrade program should ensure the facility can be used not only for testing but also for development and evaluation of tactics and operational concepts. Requirements and suggestions for achieving the capability for evaluation of EW systems in a combined Arms Army environment are provided in the following discussion:

a. Active Radars. As indicated earlier, the current number of radars which can be operated simultaneously is three. With three radars it is possible to represent a complete command link for tactical SAM systems, but realistic workloads for decision makers are difficult to achieve since each command element has only a single subordinate unit. Also, since there is only a single firing unit, the impact of disrupting command radars on the ability of firing batteries to operate autonomously cannot be evaluated. A greater capacity for simultaneous radar operation is required.

(1) The simulator should provide a capability to operate a minimum of two units at each subordinate echelon for any SAM system being used. Figure 8 illustrates this concept. Since this is a simulator facility the actual name of the threat systems are not used. The important consideration is that the facility have the hardware and software capability to develop threat scenarios such as the one shown in figure 8.

(2) The simulator should provide a capability to operate any combination of available SAM systems. This would permit simultaneous evaluation of the effects of tactics and ECM on different threat systems.

b. Aircraft Targets. Only four two-way RF paths are available to simulate aircraft targets, although a time sharing (multiplexing) capability is available on some radar simulations to permit forty targets to be represented. However, only the four targets closest (in angle)

to the victim radar's boresight can be displayed. Future testing will require increasingly larger and more complex scenarios with more jamming sources and more attack aircraft. An increased capability to represent aircraft targets, approximately 100, is required.

c. Jamming Sources. Only three one-way RF paths are available to simulate support jamming platforms, although they can be time shared to represent more than three jamming sources with some consequent loss of fidelity outside the victim radar's main lobe. However, all jammers represented in this manner are constrained to a single set of powers, gains, modulations, etc. Future testing will require combinations of standoff, standin, and escort jamming platforms, in addition to aircraft self-protection jamming, each with its own individual characteristics and parameters. An increased capability to represent support jamming sources, approximately eight to ten, is required.

d. Loading Consoles. It is impractical to envision the complete threat environment represented by RF radar simulations. However, it is necessary to represent subordinate threat systems in a realistic manner to provide a reasonable load on commanders and enhance the decision making process. Non-active radar elements can be simulated by consoles which provide an interactive capability between the operator and the threat scenario. To optimize the level of realism associated with the loading consoles, they should have the same basic capabilities inherent in the RF element they are intended to represent. Hence, through software, a firing battery would have the capability to search for, acquire, track, and engage targets. It would also be vulnerable to attack by defense suppression systems.

e. Defense Suppression. AF-EWES radar operators function in a no-threat or no-penalty environment. The effects of lethal defense suppression systems (e.g., F-4G Wild Weasel, PLSS, etc.) should be incorporated into the simulator. Several potential alternatives may be possible.

(1) Inclusion of an on-line radar engagement model which would represent the probability of site attack and the subsequent probability of damage. The radar simulation could be partially or totally disabled for the remainder of the test mission.

(2) Basic capability described above with the addition of reactive target aircraft representative of Wild Weasel hunter-killer operations. This feature would require integration of real-time knowledge of the emitter environment with a dynamic flight path generator. However, it would afford the radar operator a visual cue regarding the presence of defense suppression systems.

(3) Dynamic integration of a cockpit simulator with the threat radar environment. This would also require dynamic flight path generation, but it would permit simultaneous assessment of RWR, ECM, and tactics.

(4) Alternate approach to (3) could integrate RWR with the Test Director's Station (see paragraph v below) and permit activation of the radar engagement model in (1) by the test director or his representative.

f. Terrain Effects. The absence of terrain effects is the most serious limitation to testing of low altitude profiles and tactics. Current efforts to develop and provide appropriate ground clutter and terrain masking effects should be vigorously pursued. Terrain effects will be required on all radar simulations employed during low altitude test scenarios.

g. MEG Integration. Radar signals produced by the Multiple Environment Generator should be integrated with the threat scenario being represented. This would enable realistic evaluation of RWR's and

processors in a dynamic threat environment exhibiting the spatial relationships and emission control characteristics which would be expected. Effective model integration would be required to drive the MEG for those radars not represented by active radars or loading consoles.

h. Radar Integration. The number of specific radars which can be netted with other radars is small; not all radars can be integrated with the command and control structure. This feature should be expanded to provide the capability to represent any configuration of specific radar systems.

i. Multiplexing. The target multiplexing capability has not been incorporated into all radar simulations. This feature is required any time more than four targets are desired for testing.

j. RF Communications. The RF data links being developed for the tactical SAM systems will require expansion. The concept of loading commanders by simulating subordinate echelons using loading consoles will be degraded during ECM conditions unless two-way RF links are provided for all manned elements in the scenario.

k. Height Finders. Height finder radars are an integral part of the surveillance and acquisition functions performed by air defense elements of the Combined Arms Army. These radars should be included in the simulation. Interim workaround procedures for operators could be developed provided the approximate distribution of target position errors as a function of range, speed, altitude, aspect, etc. is known.

l. Surveillance System. The outputs of radars assigned to the early warning companies should be incorporated into the simulator. Integration of the early warning network would require a higher decision making echelon than currently exists.

m. Higher Echelon Netting. The capability to integrate at least the command elements of various threat systems should be developed. This netting would most likely occur at the Army's ADCC, and it may be possible to model this element of the system.

n. Instrumentation. The instrumentation and data handling capabilities of the simulator must keep pace with simulator development. Digital data recording should be a rule rather than an exception. Results of computer calculations completed in real-time should be retained for post-test analysis.

o. J/S Ratio Measurement. The simulator should provide a capability to determine the J/S ratio for each target aircraft as a function of radar scan. This capability is required for both noise and pulse jamming environments. Ideally, the J/S ratio would be measured at the radar receiver; as a minimum, it should be calculated and available to the test director for post-test analysis.

p. Target Identification. A strong requirement exists to be able to reconstruct a test mission/event after the fact. The current simulator configuration does not afford the user that capability. The simulator should provide the identity of each target aircraft as a function of time and location. The process of randomly assigning aircraft to target paths is inadequate, especially during conditions when unique ECM functions are being employed by a specific aircraft type. A sorting procedure is required to assign targets to RF paths in a rational and logical manner.

q. Expanded RF Head. Requirements for increased numbers of aircraft targets and jamming sources lead to a reasonable requirement to increase the capacity of the RF Head. Target multiplexing will continue to be a reasonable approach for representing large numbers of aircraft. However, multiplexing support jamming sources is not as reasonable. Also, one-way RF paths are used to represent missile downlinks and are unavailable as jamming sources at that time. The feasibility and practicability of building RF Heads with approximately four times the capacity of the current design should be investigated.

r. Timing Frame Length. The 50 millisecond time frame will probably require a change to a shorter frame length. As larger scenarios are implemented and radars with faster scan rates are employed, the probability of targets dropping during multiplexing increases. A radar with a 20 rpm scan rate will rotate through a 6-degree arc during one time frame. This represents a distance of more than 1500 meters at a range of 15 km, and it is reasonable to expect more than four aircraft within that airspace. Hence, targets will be dropped since only four can be displayed. Additionally, the simulator provides the only reasonably dense emitter environment in which to evaluate location systems such as the PLSS. However, the time difference of arrival techniques employed by the PLSS require much faster simulator operation.

s. Model Integration. There will be a continuing limitation on the threat level which can be represented in the simulator; hence, a continuing requirement exists for simulation modeling which can provide extrapolations beyond the test conditions. There are also several functions and elements within the threat environment which may be adequately represented by model outputs rather than RF simulation. Parallel development of the simulator and the computer model is required.

t. Currency. The simulator should provide the capability to evaluate ECM systems, techniques, concepts, and tactics against current and projected threat systems. Maximum advantage must be made of the secure features of the simulator to develop effective countermeasures without the typical 7-12 year lag time. In this area, the simulator should be developed to provide "capabilities" rather than the "specific threats."

u. Validation. It is imperative that simulator validation efforts conducted by the intelligence community keep pace with continuing simulator development. The true configuration of the simulator must be known at all times, and users must be aware of all deviations from the projected threat and the impact of those differences. Validation must be regarded as an integral part of development and upgrade.

IV-34

v. Test Director's Station. A single control center is required to enable the test director to monitor and manage all aspects of the test effort. Specific proposals were provided to ASD/AEW in AFTEC/OA letter dated 17 Apr 79. The station should be developed with sufficient flexibility and growth capability to permit parallel development with the simulator.

SECTION VII

SUMMARY/RECOMMENDATIONS

To briefly summarize, the test and evaluation process proposed in this paper is one which uses analytical models and hybrid laboratory simulators with field testing to achieve a more comprehensive assessment of the EW system. Hopefully, the description of the process has appeared rather straightforward, even obvious. While the concept proposed in this paper may appear obvious, the reader should not, however, be easily lulled into a belief that there is widespread acceptance of the concept. It has both intuitive and "bandwagon" appeal, but there are many obstacles to its successful implementation. There are no clearly identifiable division points in a test program; no universally recognized points at which testing stops and modeling begins. Neither is there a prescribed acceptable ratio of laboratory testing to field testing. Each EW system tends to be unique with its own particular problem areas and individual test concept. The methodology for applying the proposed concept to a specific EW system test and evaluation program must be tailored to that system. That is part of the philosophical problem with implementing the proposed concept. There are also readily recognizable problem areas with the test facilities and the analytical models.

The current EW test range facilities are not adequate to support operational testing of evolving EW systems. They do support training fairly well and, to some extent, they possess some capability to support developmental and operational testing. However, the capability is limited, and improvements are required. The test threat environment must be updated in quantity, quality, and diversity; instrumentation capabilities must be improved; and data management systems must be developed which are more flexible and more responsive to the user. Since these facilities are used by the developers and operational commands as well as the OT&E community, improvements should be based on Air Force-wide needs.

The current status of the models available to support EW system test and evaluation is, at best, difficult to determine. There is no defined plan for their development, no control of their configuration, and little or no guidance on their use or usability. Very few models have been critically reviewed, and even fewer have been calibrated against actual test data. Consequently, model outputs are not readily accepted, and the utility of models is far less than what might be possible. Potential solutions for the problem range from ignoring it to establishing an agency with total responsibility for Air Force modeling. It is unlikely that either of these extremes would be effective. However, as a minimum, some sort of library should be established to provide the current status or configuration of an "accepted" group or family of models. Criteria for acceptance must still be established, but acceptability should at least be based upon correlation with empirical test data.

Finally, the hybrid man-in-the-loop simulators are the area most needing a firm hand. It is clear that with cut backs in flying hour allocations, flying time available for testing and concept and tactics development is going to be adversely impacted. Flying cut backs should make the use of hybrid simulators even more important. Consequently, improvements to facilities such as AFEWES should be based on a master plan developed by all the potential users rather than come as a result of uncoordinated, but frequently related, demands from a number of programs. The list of improvements discussed in section VI of this report provides a basis for developing a master plan for AFEWES.

As stated earlier, implementation of this concept will not be easy. A strong Air Force program is required to improve facilities and establish procedures. Developers, testers, and users must all be involved in the process of determining what is to be done and how it is to be accomplished. That means actively participating in planning test facility development, as well as sharing the recurring operating costs of those facilities. It is possible to accomplish more comprehensive test and evaluation of evolving electronic warfare systems. It is possible to develop tactics and operational employment concepts more efficiently. It is possible to address the decision maker's questions more completely

than in the past. It is possible to establish an unprecedented level of credibility in the electronic warfare systems test and evaluation process. It is all possible--but it does require an Air Force commitment.